「通訊傳播事業個資法遵教育及實務案例分享」

謝淯婷 法律研究員/律師

資策會科技法律研究所

2024.05.03

stli 科技法律研究所 SCIENCE & TECHNOLOGY LAW INSTITUTE

大綱

1. 個人資料保護法重點條文(含修正重點)及法律效果與責任
2. 個人資料保護管理機制(規劃、執行、檢查及改善)及個人資料保護法第8條之告知義務
3. 個資管理機制之實務案例解析分享(含事故責任)

為什麼需要個資法？

個資外洩頻傳，個人資料保護意識抬頭

即時 政治 國際 兩岸 產經 證券 科技 生活 社會 地方 文化 運動 娛樂 影音 專題 媒體識讀

首頁 / 國際

AT&T用戶個資外洩 估影響7300萬人

2024/3/31 05:49（3/31 07:42 更新）

美國電信巨擘AT&T商標。（路透社）

（中央社達拉斯30日綜合外電報導）美國電信巨擘AT&T今天宣布，已開始向數以百萬計的客戶通報近日發現的個人資料遭竊事件，影響範圍可能超過7300萬名用戶。

美聯社報導，AT&T正調查約2週前在「暗網」上發布的一個資料集。初步分析顯示，這個資料集包含約760萬現有用戶和6540萬前用戶的社會安全號碼等個資。

該公司表示，已重新設定現有用戶的密碼，並將與敏感個資遭外洩的用戶進行溝通。

AT&T透過聲明指出，目前尚不清楚這些個資是「源自AT&T或其供應商之一」。資料集似乎來自2019年或更早，內容涵蓋用戶密碼、社會安全號碼以及電郵信箱、電話號碼、出生日期等資訊，但不包括財務資訊或通話紀錄。

今年2月，總部位於達拉斯的AT&T也曾因斷電曾導致數千名美國用戶的手機服務中斷。當時AT&T將此事歸咎於技術問題，而非惡意攻擊。（譯者：施施）1130331

#AT&T #美聯社 #美國 #個資

https://www.cna.com.tw/news/aopl/202403310005.aspx 1/3

yahoo! 新聞

焦點 地震防災 即時 娛樂影劇 國際 政治 社會地方 財經 運動 玩樂 品味 健康 遊戲3

台視新聞網 | 5.7k 人追蹤 ☆ 追蹤

7所高中校務系統遭駭！ 多達2萬筆個資外洩

台視新聞網
2024年4月1日

日前，有學校的校務行政系統遭到駭客入侵，教育部再追蹤發現，全台有7所高中使用亞昕資訊公司的校務行政系統，3月中部分學生的個資遭到駭客散布後，外洩的資料地址大多分布在中彰投，還有1988年和1989年出生者，甚至連家長姓名、電話全都被曝光，資料多達2萬筆。目前教育部已啟動資安事件通報等應變措施，也通知個資被外洩的當事人，更請學校注意學生資料有無被盜用。

「亞昕資訊」遭勒索拒付款 駭客外洩學生個資

提供個人資料給學校，但萬萬沒想到校務行政系統居然會被駭客入侵。事件曝光後，教育部後續追蹤發現，全台包含桃園、苗栗、台中等7所使用「亞昕資訊公司」校務行政系統的高中，都遭到駭客入侵。

而駭客取得個資後，先是向公司勒索贖款，亞昕公司拒付後，駭客就外洩學生個資，而遭到外洩的資料地址大多分布在中彰投，1988年和1989年出生者，甚至連家長姓名、電話全都被曝光，資料多達2萬筆！

熱門新聞

1. 徐國勇女兒低調卻遭起底！林楚茵直指「兇手」：就是徐巧芯！
2. 民眾以為最多1個月 哀喊「等這麼久」
3. 兒子原單這備註「媽媽是婊子」！她拐率發過程：不會提告
4. 花蓮山海戲大樓「強震裂成X形」住戶拒拆！網拐辛酸原因
5. 留缺別率記...高雄小五女童一早肖害包上頂樓墜亡 校方：她人緣很好

你可能會喜歡

https://tw.news.yahoo.com/7所高中校務系統遭駭-多達2萬筆個資外洩-070227970.html 1/11

新聞中的個資外洩事件

有關和雲行動服務iRent發生用戶個資外洩事件查處說明

資料來源：交通部公路總局-秘書室-公關科
聯絡人：運輸組綜合運輸科 梁郭國組長
聯絡資訊：02-2307-0123轉3999

分類	監理
公告日期	112-02-09 09:45
公告單位	交通部公路總局-秘書室-公關科
內容	有關和雲行動服務股份有限公司(iRent) 發生用戶個資外洩一事，經本局於2月4日派員至該公司進行稽查，確認該公司未依「個人資料保護法」與「汽車運輸業個人資料檔案安全維護計畫及處理辦法」採行適當之安全措施致個人資料洩漏，又未訂定完整個人資料檔案安全維護計畫，且因該公司屆期仍未改正，發生外洩風險之個資筆數達40萬筆，情節重大，已明確違反個人資料保護法第27條第1項及第2項規定，爰依個人資料保護法第48條第4款規定處最高罰鍰新臺幣20萬元，本局已要求業者落實個人資料保護法相關規定，並於2月28日前提送完整改正佐證資料，倘後續查有違反個人資料保護法情事，將按次處以罰鍰。 本局將持續督促汽車運輸業者落實用戶個資維護及企業社會責任，以保障消費者權益。

近年常見重大個資/資安事件

公部門、關鍵基礎設施

2018.4	高雄果菜公司	駭客資料勒贖
2018.12	台灣高鐵	高鐵票務系統被駭
2019.1	台北市衛生局	298萬筆市民個資外流
2019.6	銓敘部	59萬筆公務員個資外流
2020.5	中油、台塑	駭客癱瘓支付與內部系統
2022.08	臺灣政府網站	相關機構遭到大量的網路攻擊
2022.10	內政部戶政資料	駭客在暗網兜售2357萬筆戶役資料
2023.1	華航	駭客勒贖、會員個資外洩
2023.3	故宮	數千件國寶圖檔遭竊賤賣

金融機構

2016.7	第一銀行	東歐駭客入侵盜領8327萬元
2017.2	13家證券公司	首起集體遭駭客勒索
2017.1	遠東銀行	被盜轉6010萬美元
2021.11	7家券商、1家期貨商	駭客撞庫攻擊、客戶被異常下單
2022.6	12家券商、期貨商	中華電信BGP發現異常，啟動中斷機制
2023.11	上海商銀	1.4萬客戶資料外洩
2024.1.18	法商法巴人壽及法巴產險	未經金管會核可進行雲端委外作業

科技業

2018.8	台積電	生產線停擺、營收損失達52億
2019.3	廣達	東歐駭客冒名詐取貸款
2019.3	華碩	軟體更新檔被入侵影響上萬台電腦
2020.11	鴻海、仁寶、研華	駭客資料勒贖
2021.4	宏碁等多間科技廠	勒索軟體攻擊
2022.2	竹科7家半導體廠商	陸駭客展開持續性滲透威脅（APT）行動
2023.3	宏碁	廠商密碼保存與管理不當，遭到無權限者非法使用

民生消費

2022.11	雄獅旅行社	不法人士假冒其名義、利用半年內訂單資訊進行詐騙
2023.1	iRent	資料庫未加密40萬筆個資外洩
2023.2	微風	90萬筆個資外洩
2023.5	微笑單車	透過境外IP位址嘗試取得YouBike的會員帳號、密碼
2023.5	誠品、蝦皮	蝦皮及誠品生活未依個資法採行適當之安全措施，屆期未改正
2023.11	LINE日本母公司	外包公司員工的電腦感染惡意軟體，系統遭到不當存取

整理自聯合報系列報導：全民遇駭紀實

個資法立法目的

個資法§1	為規範個人資料之蒐集、處理及利用，以**避免人格權受侵害**，並**促進個人資料之合理利用**，特制定本法

個資法立法精神

個資法 §5	個人資料之蒐集、處理或利用，應尊重當事人之權益，依**誠實及信用**方法為之，不得逾越**特定目的**之**必要範圍**，並應與蒐集之目的具有**正當合理**之關聯

- 何謂比例原則？

國家發展委員會108年3月27日發法字第1080005819號函

- 貴局來函固稱蒐集旅客登記資料之目的係為查察色情媒介與違法擴大營業，惟查察色情媒介部分，**是否需要蒐集所有旅客之登記資料**，抑或可依據貴局彙整之可疑特徵，自登記資料中挑選出以一人或一個代號連續入住多房多天之對象為蒐集
- 又查違法擴大營業部分，是否需要蒐集旅客詳細之登記資料，抑或可透過統計資料之比對，佐證實際經營與登記經營之房間數量是否一致。是以倘全面性蒐集所有旅客之登記資料而逾特定目的之必要範圍，恐有違反比例原則

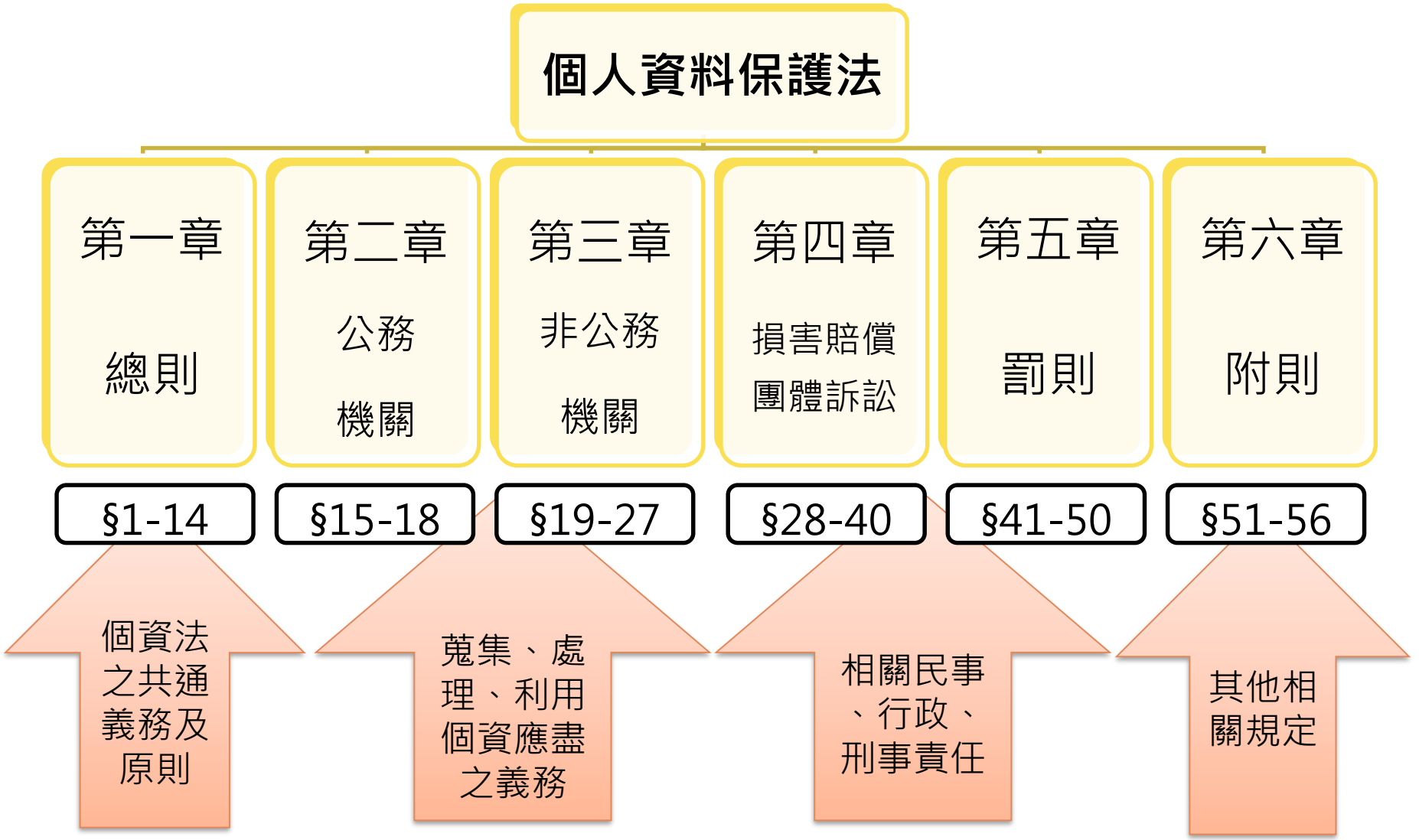
個資蒐集目的內利用與比例原則

● 國家發展委員會發法字第1090011600號

有關衛福部函詢「提供兒童及少年施用毒品個案資料送警察機關列為關注對象，以利警察人員溯源追查供毒網絡」，是否符合個資法？

- 「社會安全網-關懷e起來通報平台」所蒐集之施用毒品等兒少個案資料，原係為協助兒少後續就醫、保護、安置或為其他必要處置，如將相關資料做上述目的外之利用，使原應受保護、關懷之兒童少年成為警察機關之關注對象，除可能妨礙兒少權益保障之原始目的達成外，亦與個人資料之利用應符合誠實信用方法之原則有間，**尚難認符合個資法第5條之規定**
- 又警察機關如有其他替代之偵查手段，則提供相關資料之必要性亦將有疑義，恐難符合同法第16條但書第2款「為維護國家安全或增進公共利益『所必要』」之規定

個資法之架構



什麼是個人資料？

個資法第2條第1款對個人資料有所定義

個人資料分為一般個資及特種個資

- **個資法第2條第1款：**

個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料

- **個資法第6條第1項(特種個資原則不得蒐集、處理、利用)：**

有關**病歷、醫療、基因、性生活、健康檢查及犯罪前科**之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：……

一般個資：姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、聯絡方式、財務情況、社會活動
※概括條款：其他得以直接或間接方式識別該個人之資料
特種個人資料：病歷、醫療、基因、性生活、健康檢查、犯罪前科

蒐集、處理、利用？

個資法第2條第3至5款分別就蒐集、處理、利用有所定義

蒐集

指以任何方式取得個人資料

處理

指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送

利用

指將蒐集之個人資料為處理以外之使用

如：依據顧客所留之地址資料來遞送貨物，或依客戶資料檔案所留電話號碼進行資訊聯繫等行為，均屬於對個人資料之利用

公務機關蒐集、處理要件

個資法第15條規範公務機關之蒐集、處理應有特定目的，且應符合特定情形

● 個人資料保護法§15

公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有**特定目的**，並符合下列情形之一者：

一、執行法定職務必要範圍內

- 警察根據法律負有戶口查察、犯罪預防等法定職務，因此為了執行職務之特定目的，在必要範圍內，警察即可針對轄內居民進行家戶訪查，詢問戶內人口狀況（蒐集），並加以記錄（處理）。但是如蒐集或處理超出其法定職務必要範圍，則仍為法所不許

二、經當事人**同意**

三、對當事人權益無侵害

非公務機關蒐集、處理要件

個資法第19條規範非公務機關之蒐集、處理應有特定目的，且應符合特定情形

- **個人資料保護法§19**

非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有**特定目的**，並符合下列（**八款**）情形之一者：

一、法律明文規定。

二、**與當事人有契約或類似契約之關係，且已採取適當之安全措施。**

三、當事人自行公開或其他已合法公開之個人資料。

四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。

五、經當事人**同意**。

六、**為增進**公共利益**所必要**。

七、個人資料取自於一般可得之來源。**但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。**

八、對當事人權益無侵害。

- 蒐集或處理者知悉或經當事人通知依前項第七款但書規定禁止對該資料之處理或利用時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。

非公務機關蒐集、處理要件試舉例

一、法律明文規定

- 「人工生殖法」第14條規定，醫療機構實施人工生殖，應載明受術夫妻之姓名、住（居）所、國民身分證統一編號或護照號碼、出生年月日、身高、體重、血型、膚色及髮色等

二、與當事人有契約或類似契約之關係，且已採取適當之安全措施

- 個資法施行細則第27條第1項規定，是指與當事人間有買賣契約、僱傭契約或委任契約等法律關係

三、當事人自行公開或其他已合法公開之個人資料

- 個資法施行細則第13條。個人資料已由當事人自行公開或已合法公開者，對於這類個人資料進行蒐集或處理，不至於侵害當事人權益，故為個資法所允許之合法情形之一

四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人

- 學術機構為了統計我國三十歲以上男性因肺癌死亡之機率，且無法識別特定當事人

非公務機關蒐集、處理要件試舉例

五、經當事人同意

- 須履行告知義務，並留下同意書

六、為增進公共利益所必要

- 新聞媒體為保障人民知的權利，監督政府施政，而於合理範圍內蒐集個資

七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限

- 個資法施行細則第28條

八、對當事人權益無侵害

- 新任職員或公司客戶提供緊急聯絡人資料

非公務機關蒐集、處理要件

就員工及消費者資料之蒐集，應符合個資法第19條所規範之情形方屬個人資料之合法蒐集

- 員工：
  - 法律明文規定-**勞動基準法第7條**
  - 契約或類似契約關係，且已採取適當安全維護措施
  - 經當事人同意
- 消費者：
  - 契約或類似契約關係，且已採取適當安全維護措施
  - 經當事人同意

特種個資之蒐集、處理及利用限制

特種個資依個資法第6條第1項之規定，原則不得蒐集、處理、利用應符合例外情形方得為之

- **個資法§6 I**

有關**病歷、醫療、基因、性生活、健康檢查及犯罪前科**之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：

一. 法律明文規定

二. 公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施

三. 當事人自行公開或其他已合法公開之個人資料

四. 公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人

五. 為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施

六. 經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限

特種個資之例外試舉例

- **個資法§6 I**

一. 法律明文規定

- 職業安全衛生法第20條第1項，雇主於僱用勞工時，應施行體格檢查；對在職勞工應施行下列健康檢查

二. 公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施

- 傳染病通報

三. 當事人自行公開或其他已合法公開之個人資料

- 臉書上的自我介紹欄公開姓名、電話、照片等資訊

特種個資之例外試舉例

- **個資法§6 I**

四. 公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人

五. 為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施

- 檢警機關向醫院調閱犯罪嫌疑人的病歷資料作為犯罪偵察之用。

六. 經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限

個資蒐集、處理、利用要件彙整

個資法§15 公務機關	個資法§19 非公務機關	個資法§6 特種個資
執行法定職務必要範圍	法律明文規定	法律明文規定
經當事人同意	經當事人同意	公務機關執行法定職務或非公務機關履行法定義務必要範圍內
對當事人權益無侵害	對當事人權益無侵害	為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內
	當事人自行公開或其他已合法公開之個人資料	經當事人*書面同意
	學術研究機構基於公共利益為統計或學術研究而有必要	當事人自行公開或其他已合法公開之個人資料
	與當事人有契約或類似契約關係	公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要
	為增進公共利益所必要	
	個人資料取自於一般可得之來源	

且事前或事後有適當安全維護措施

*但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限

個資的目的外利用要件彙整

個資法§6

- 一、法律明文規定
- 二、公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施
- 三、當事人自行公開或其他已合法公開之個人資料
- 四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人
- 五、為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施
- 六、經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限

個資法§16、20

- 一、法律明文規定
- 二、為（維護國家安全或）增進公共利益所必要
- 三、為免除當事人之生命、身體、自由或財產上之危險
- 四、為防止他人權益之重大危害
- 五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人
- 六、經當事人同意
- 七、有利於當事人權益

個資法施行後再次修正

2010.04.27	2010.05.26	2012.09.26	2012.10.01	2015.12.30	2016.03.15	2023.05.31
個人資料保護法三讀通過	總統令公布個人資料保護法	施行細則正式公告	個人資料保護法正式施行	個人資料保護法修正	個人資料保護法修正條文暨細則施行	個人資料保護法增修部分條文

個資母法>>>施行細則>>>各機關辦法>>>行業標準

行為規範
新增特種個資病歷&例外特定情形

行為規範
同意不再侷限於「書面同意」

行為規範
增、修訂免告知事由&法定情形

行為規範
間接蒐集告知義務

責任內涵
與意圖營利相關之刑責修正

主管機關&適用辦法者之認定

- 詳法務部個資法非公務機關之中央目的事業主管機關列表
- 國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法§2

一、電信事業

二、用戶數達三千戶以上之提供網際網路接取服務之設置未使用電信資源之公眾電信網路者

三、有線廣播電視系統經營者

四、電視事業

五、訂戶數達三千戶以上之直播衛星廣播電視服務事業

六、經營國內新聞台頻道或購物頻道之衛星或他類頻道節目供應事業

七、電信消費爭議處理機構

八、其他經國家通訊傳播委員會（以下簡稱本會）公告之通訊傳播事業

個資檔案安全維護規範現況-2024年

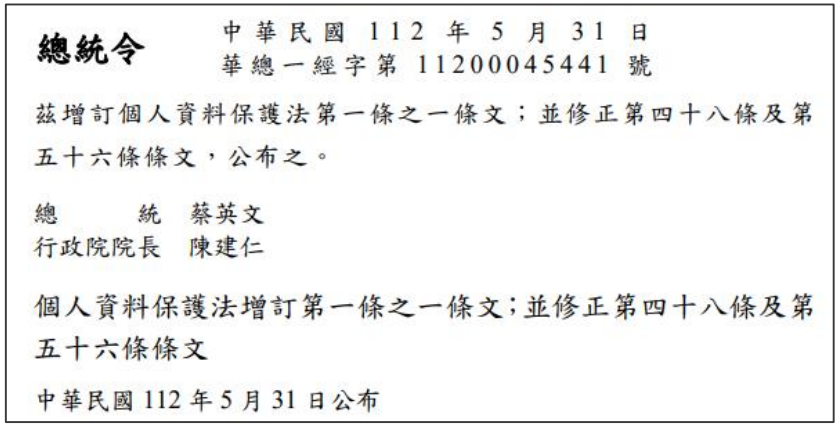
統計截至2024/04

主管機關	業別	辦法數
數位部	數位經濟相關產業（包含：電子購物及郵購業 、軟體出版業 、電腦程式設計、諮詢及相關服務業、資料處理、主機及網站代管服務業、其他資訊服務業，以及其他資訊服務業 ）	1
經濟部	綜合商品零售業、製造業及技術服務業、自來水事業、電業及公用天然氣事業、著作權集體管理團體	5
金管會	金融控股、銀行、證券、期貨、保險、電子支付、其他經金管會公告之金融服務業、財團法人	1
通傳會	電信事業、用戶數達三千戶以上之提供網際網路接取服務之設置未使用電信資源之公眾電信網路者、有線廣播電視、電視、訂戶數達三千戶以上之直播衛星廣播電視服務事業、經營國內新聞台或購物頻道事業、電信消費爭議處理機構及其他公告通傳事業等八類	1
交通部	民用航空運輸業、船舶運送業、汽車運輸業、交通部指定非公務機關（觀光旅館業、旅館業、民宿、旅行業、觀光遊樂業）、停車場經營業	5
教育部	短期補習班、私立兒童課後照顧服務中心、私立專科以上學校及私立學術研究機構、私立高級中等以下學校及幼兒園、運動彩券業、海外臺灣學校及大陸地區臺商學校	6
內政部	交友服務業、殯葬服務業、營建類非公務機關、移民業務機構、祭祀團體、政黨及全國性民政財團法人、宗教團體、地政類非公務機關、合作及人民團體類非公務機關、警政類非公務機關	10
勞動部	私立職業訓練機構、人力供應業、人力仲介業	3
衛福部	醫院、精神復健機構、私立長期照顧服務機構、護理機構、社會福利機構、中藥批發零售業、化粧品批發零售業、醫療器材批發零售業、西藥批發零售業、非輻射電子醫療器材設備製造業、食品業	11
財政部	報關業、保稅倉庫物流中心、記帳士與記帳及報稅代理人、菸酒事業、公益彩券發行機構	5
公平會	多層次傳銷業	1
工程會	工程技術顧問業	1
核安會	游離輻射設備製造業	1
中央銀行	票據交換所	1
農委會	農藥販賣業、農業金融	2
陸委會	大陸委員會指定非公務機關	1
僑委會	僑務委員會指定特定非公務機關	1
合計		56

總統 5/31 公布修正個資法

2023年個資法修法歷程

行政院提出草案	委員會審議完畢	立法院三讀通過	總統公布生效
2023/04/13	2023/05/03	2023/05/16	2023/05/31



總統令　中華民國 112 年 5 月 31 日
華總一經字第 11200045441 號

茲增訂個人資料保護法第一條之一條文；並修正第四十八條及第五十六條條文，公布之。

總　　統　蔡英文
行政院院長　陳建仁

個人資料保護法增訂第一條之一條文；並修正第四十八條及第五十六條條文

中華民國 112 年 5 月 31 日公布

修正重點

- 增訂§1-1：增設個資專責機關
- 修正§48：加重未採安全措施之處罰

為何需要個資專責機關？

同一公司所涉及不同業務之主管機關不同，造成實務遵循混亂，專責機關則得統一管轄

藥品及醫用化學製品製造業

行政院主計總處分類代碼 200

經濟部
【中藥製造業】：衛生福利部
【其餘藥品及醫用化學製品製造業】：衛生福利部

餐館業或飲料店

行政院主計總處分類代碼 561

【飯店、觀光旅館、機場附屬之餐館業】：交通部
【百貨業附屬之餐館業】：經濟部
【其他餐館業】：衛生福利部

請詳：個資法非公務機關之中央目的事業主管機關列表

個資專責機關

將設立個資委員會，籌備處已於去年12月設立

個資法新增第1條之1

變動項目	舊法	新法	差異
主管機關	各中央目的事業主管機關、地方政府	個人資料保護委員會（尚未設立/層級未定）	轉為集中監理

個資保護委員會成立後，各中央目的事業主管機關、地方政府權責，移交個資保護委員會管轄

後續需關注項目

- 個資保護委員會層級、設立時程
- 監督事權統一方式

加重未採安全措施之處罰

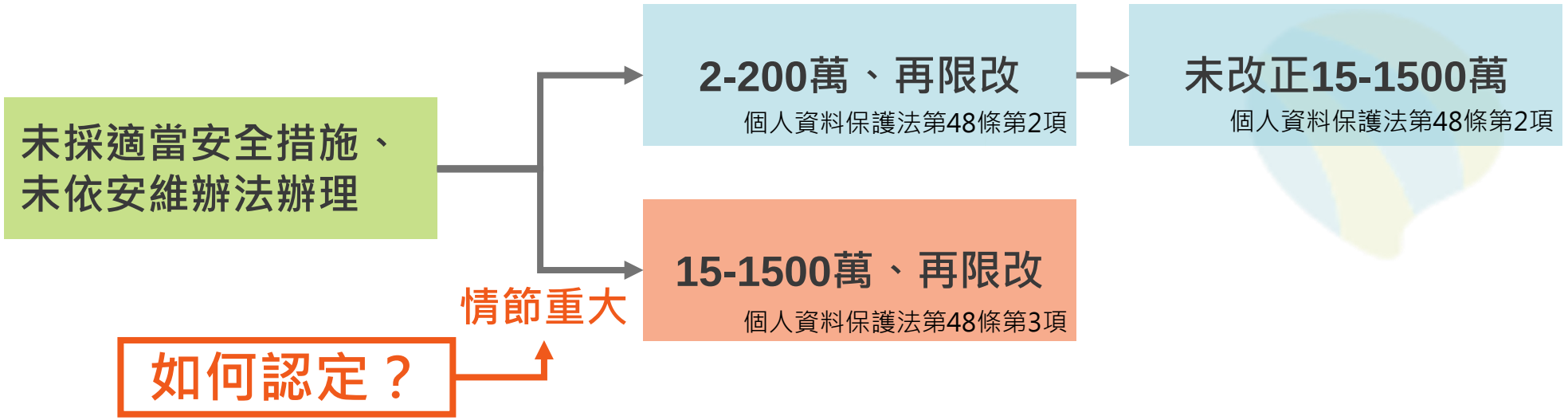
加重未有適當安全措施處罰，取消需先限改規定

個資法第48條新增第2項、第3項規定

違反項目	舊法	新法	差異
違反告知義務、當事人權利行使、行銷規定 48條1項	先限期改正， 未改正2-20萬	先限期改正， 未改正2-20萬	不變
未採適當安全措施、未依安維辦法辦理 新增48條第2、3項	先限期改正， 未改正2-20萬	● **2-200萬、再限改 未改正15-1500萬** ● **情節重大： 15-1500萬、再限改**	**罰則提高 無需先限改**
代表權人兩罰規定 50條	除盡防止義務外， 受同一處分	除盡防止義務外， 受同一處分	**罰則 實質提高**

按行政罰法第19條，僅法定罰鍰最高3,000元以下者，方得以其情節輕微免予處罰
若主管機關認定非公務機關違反個資法第27條規定，未採取適當安全措施，
則主管機關仍須依法處分

新個資法48條3項情節重大認定標準



國家發展委員會「個人資料保護法第四十八條第三項『情節重大者』認定之參考原則」

1) **個資外洩情形**：個資類別、人數、影響程度、故意或重大過失
2) **安全維護措施落實情形**：有無落實個資法第27條第3項、是否造成個資外洩
3) **知悉個資外洩後採行措施**：有無採取降低損害行為、通報、配合行政檢查、通知
4) **其他**：未遵循主管機關處分、因個資外洩獲益

國發會『情節重大者』認定之參考原則

- 主管機關得綜合考量非公務機關之下列情形：

(一) **個人資料外洩情形**：

1、 所涉個人資料類別是否包含本法第六條所稱「病歷、醫療、基因、性生活、健康檢查、犯罪前科」等**特種個人資料**

2、 所涉及當事人之**人數多寡**

3、 外洩行為對於當事人所生之**影響程度**

4、 外洩是否出於**故意或重大過失**

(二) **安全維護措施之落實情形**：

1、 有無依本法**第二十七條第三項**所定辦法規定，採取安全維護措施

2、 是否曾因未盡個人資料安全維護義務，而有**發生個人資料外洩情事**

(三) 知悉個人資料外洩後採行措施：

1、 有無採取**降低當事人損害**之行為

2、 有無依規定主動**通報**主管機關

3、 有無**規避、妨礙或拒絕**主管機關**調查**之情事

4、 有無以適當方式**通知**當事人

(四) 其他：

1、 是否**遵循主管機關**依本法規定就同一個人資料外洩案件所為之**相關處分**

2、 是否因該個人資料外洩**獲有直接或間接之利益**

(五)行政罰法第18條：

裁處罰鍰，並**得考量受處罰者之資力**

PIMS 個資保護管理制度的重要性

PIMS個資保護管理系統

ISMS資訊安全管理系統

組織文化

技術面

風險管理

細節面

ISMS著重於技術及細節面，PIMS更強調組織文化及風險管理方法論。
舉例而言，**即使企業資訊化及數位化程度較低，於日常業務仍可能涉及員工或客戶個資保護處理議題**。

什麼是TPIPAS？

經濟部

TPIPAS

臺灣個人資料保護與管理制度

導入TPIPAS—培訓內部人才

dp.mark 資料隱私保護標章

驗證—取得標章

moda 數位發展部 Ministry of Digital Affairs

唯一政府建置及推動的個資保護制度

2010年 為完善國內商務交易安全環境，在經濟部商業司的委託下，資策會科技法律研究所(科法所)自起建置及推動「臺灣個人資料保護與管理制度」（TPIPAS）

2017年 受經濟部委託，資策會持續擴大維運經濟部隱私標章

2019年 資策會辦理TPIPAS十年有成，受國發會青睞及力薦，於2019年7月指定**資策會以TPIPAS為基礎，向APEC提出當責任機構**（Accountability Agent, AA）

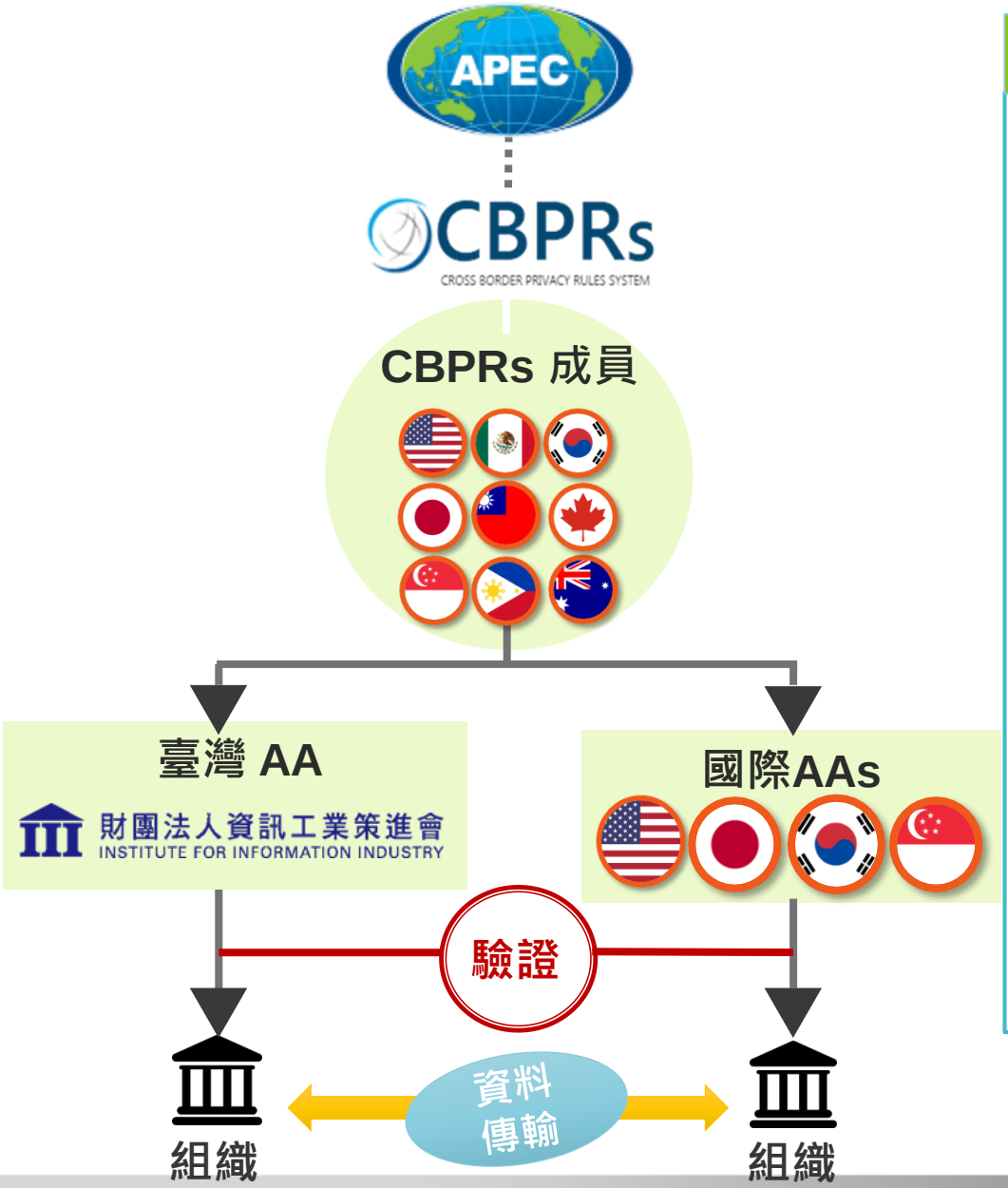
2021年 資策會**獲准成為亞太經濟合作跨境隱私規則體系當責機構**。我國成為第5個擁有當責機構的APEC會員體

2022年 TPIPAS個資業務移轉數位部

國際PIMS標準概述

	類別	相關法律	組織
ISO27001	資訊安全管理系統	N/A	**ISO**
ISO27701	個人資料管理系統	GDPR	**ISO**
BS10012	個人資料管理系統	GDPR	**BSI**
TPIPAS	個人資料管理系統	我國個資法	**資策會**
CBPR	個人資料管理系統	N/A	**APEC**

跨境隱私規則體系（CBPRs）介紹



唯一亞太地區認可之驗證標準

- CBPR是國際級驗證，為我國政府參與推動數位經濟發展基礎重要的一環
- CBPR透過參與的APEC會員體共同建立國際隱私法遵一致性的要求，並藉由各國指定之當責機構（Accountability Agent, AA）對企業進行驗證
- CBPR可證明企業或組織對資料或個資管理的重視與能力，建構合規資料自由流通的信賴環境，促進商務貿易往來
- 透過TPIPAS及CBPR驗證，檢視企業在資料蒐集流程，進而改善內部資料創新

CBPRs ⟷ TPIPAS

CBPRs CROSS BORDER PRIVACY RULES SYSTEM

TPIPAS 臺灣個人資料保護與管理制度

CBPR+TPIPAS最符合國內外個資法要求

制度	CBPR	TPIPAS	BS 10012	ISO 27001	ISO 27701
性質	國際隱私法遵標準	個人資訊管理系統（PIMS	個人資訊管理系統（PIMS	資訊安全管理系統（ISMS	擴充27001增加對資訊安全管理要求
主導單位	APEC	我國數位部	英國標準協會	國際標準組織	
特色	以國際要求銜接各國法遵規範，建立國際性一致性標準	● 唯一依照我國個人資料保護法為基礎設計 ● 銜接APEC CBPR國際要求	● 僅適用英國境內 ● 主要依循GDPR設計	第一個全球資訊安全管理的國際標準	包括：ISO27001ISO27002 ISO29100
所涉法令	國際法	我國個資法	GDPR	無法律基礎	無法律基礎

CBPR VS. ISO27701基本介紹

	APEC CBPR	ISO/IEC 27701：2019
簡介	亞太經濟合作（APEC）為促進會員體間資料流動提供之跨境隱私規則（CBPR）	ISO 27701 隱私資訊管理為 27001 資訊安全管理系統及 27002 資訊安全控制措施擴展
特色	• 以**個資隱私保護**為主，著重跨境資料傳輸 • 國際間隱私保護能力之有力證明	• 於**資安基礎**上，加強個資保護 • 必須藉由延伸ISMS（ISO/IEC 27001）驗證，**不能獨立獲得**
法律效力	為國際**法律**性質	為國際**標準**性質
官方監管	APEC DPS JOP	無
標章效期	要求**每年更新一次**	要求每三年更新一次
申請時間	1～3個月	3～6個月

- **CBPR**透過法遵標準框架，讓會員體可依據CBPR調整國內個資法令，並由各國對內要求執行與約束。其精神在於**融合國際法遵標準的同時因地制宜**，尊重各國法規體系的特色。
- **ISO27701**建基於ISO27001與ISO27002所頒佈之資安標準。與CBPR最大的差異係ISO27701屬產業自律選擇之標準，**並無官方監管單位、不具法律直接效力**。

個資保護管理機制法規層面要求

國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法
針對該辦法適用之非公務機關主要有四大要求

§3
適當安全措施要求、個資檔案安全維護計畫訂立

§4
個資事故應變、通報及改善機制建置

§5
個資管理程序訂定

§6
相關紀錄、證據保存機制訂定

適當安全措施之要求

- 個人資料保護法§27

➢非公務機關保有個人資料檔案者，應採行**適當之安全措施**，防止個人資料被竊取、竄改、毀損、滅失或洩漏

➢中央目的事業主管機關得指定非公務機關訂定**個人資料檔案安全維護計畫**或業務終止後個人資料處理方法

➢前項計畫及處理方法之標準等相關事項之辦法，由中央目的事業主管機關定之

- 國家通訊傳播委員會指定非公務機關個人資料檔案安全維護辦法(下稱個資檔案安全維護辦法)§3第1項

非公務機關應依其業務規模及特性，衡酌經營資源之合理分配，配置管理之人員及相當資源，以規劃、訂定、修正與執行其**個人資料檔案安全維護計畫**及**業務終止後個人資料處理方法**

何謂適當安全措施？(1/2)

- **臺灣新竹地方法院108年度小上字第29號民事判決**

  - 上訴人所提之個資法施行細則第12條第2項所列舉之11款，僅為規範非公務機關所採行之適當安全措施所「得」包括之事項，並非必定應含事項，縱使非公務機關所採取之安全措施事項未依照此等規範，亦非當然可得認定其未踐行個資法第27條第1項所定之義務，是上訴人此部分指適原判決違背法令，亦非有理

何謂適當安全措施？(2/2)

- **個人資料保護法施行細則第12條2項**

所謂適當安全措施，**得**包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：

一、配置管理之人員及相當資源

二、界定個人資料之範圍

三、個人資料之風險評估及管理機制

四、事故之預防、通報及應變機制

五、個人資料蒐集、處理及利用之內部管理程序

六、資料安全管理及人員管理

七、認知宣導及教育訓練

八、設備安全管理

九、資料安全稽核機制

十、使用紀錄、軌跡資料及證據保存

十一、個人資料安全維護之整體持續改善

適當安全措施例示

物理防護

- 門禁管理
- 錄影監控
- 識別證
- 全程陪同訪客
- 謹防尾隨事件

主機

- 異常行為分析
- 使用者權限

資料庫

- 軌跡監控與稽核
- 異常行為分析
- 使用者權限

內部員工

- 上網行為
- 電子郵件
- 通訊軟體
- 可攜式儲存媒體
- 非法軟體檢查

其他

- 防毒軟體
- 程式更新
- 無線網路掃描

個人資料檔案安全維護計畫訂立(1/3)

- 個資檔案安全維護辦法§3
  - 非公務機關應依其業務規模及特性，衡酌經營資源之合理分配，配置管理之人員及相當資源，以規劃、訂定、修正與執行其個人資料檔案安全維護計畫及業務終止後個人資料處理方法（以下簡稱本計畫及處理方法）
  - 本計畫及處理方法之**訂定或修正**，**應經**非公務機關**負責人或法定代理人簽署**
  - 非公務機關蒐集、處理及利用達**五千名用戶**之個人資料者，其訂定之本計畫及處理方法內容應包含**國內或國際個人資料安全稽核機制之規劃及執行計畫**

個人資料檔案安全維護計畫訂立(2/3)

- **公司基本資料、安全維護計畫目的**
- **個人資料檔案之安全維護管理措施：**
  - **配置管理之人員及相當資源**(個資檔案安全維護辦法§3)
  - **事故之應變、通報及改善機制**(個資檔案安全維護辦法§4)：
    - 應採取之應變措施：控制當事人損害方式、事故通知之適當方式及內容
    - 事故應受通報之對象及方式
    - 改善措施之研議機制
  - **個人資料之管理程序**(個資檔案安全維護辦法§4)
    - 是否符合個資法第6條規定(特定目的)
    - 是否有免為告知事由、告知之內容及方式是否合法妥適
    - 是否符合個資法第19條規定(特定目的)、第7條規定(當事人同意)
    - 是否符合蒐集之目的必要範圍、目的外利用是否符合法定情形
    - 當事人拒絕行銷立即停用、首次行銷提供免費表示拒絕接受方式
    - 委外監督適當監督並於委託契約明確約定
    - 國際傳輸是否有法令限制
    - 個資法第3條當事人權利行使相關事項
    - 檢視個資正確性及若有不正確或爭議之處理
    - 個資特定目的消失或期限屆滿檢視
    - 當事人申訴諮詢管道

個人資料檔案安全維護計畫訂立(3/3)

- **資料檔案之安全維護管理措施(續)：**
  - **相關紀錄、證據保存機制**(個資檔案安全維護辦法§6)：
    - 所紀錄之個人資料使用情況、軌跡資料及相關證據
    - 刪除、停止處理個資後所留存：
      - ■刪除、停止處理或利用之方法、時間
      - ■若將刪除、停止處理或利用個資移轉至其他對象時，移轉原因、對象、方式、時間，及該對象蒐集、處理、利用之合法依據

Q 未訂立個資檔案安全維護計畫？

A 個資法第48條第2項

非公務機關違反第二十七條第一項或**未依第二項訂定個人資料檔案安全維護計畫**或業務終止後個人資料處理方法者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣**二萬元以上二百萬元以下罰鍰**，並令**其限期改正，屆期未改正者**，按次處新臺幣**十五萬元以上一千五百萬元以下罰鍰**

個資事故應變、通報及改善機制之建置

- 個資檔案安全維護辦法§4第1及第2項

非公務機關為因應**個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故**（以下簡稱事故），應訂定下列**應變、通報及改善機制**：

一、事故發生後應採取之應變措施，包括控制當事人損害之方式、查明事故後通知當事人之適當方式及內容

二、事故發生後應受通報之對象及其通報方式

三、事故發生後，其改善措施之研議機制

非公務機關遇有重大個人資料事故者，應於**知悉後一小時**內通報本會，並於**七十二小時**內依附表格式，**續行通報本會**。但非公務機關接獲本會或有關機關通報發生事故時，應於四十八小時內，依附表格式通報本會

第四條 附表 **個人資料侵害事故通報紀錄表**

個人資料侵害事故通報紀錄表		
非公務機關名稱 ＿＿＿＿＿＿	通報時間：　年　月　日　時　分 通報人： 職稱： 電話： 電子郵件： 事故地址：	
事故發生時間		
事故發生種類	□竊取 □洩漏 □竄改 □毀損 □滅失 □其他侵害事故 ＿＿＿＿＿＿	個資侵害之總筆數(大約) ＿＿＿＿＿＿ □一般個資＿＿＿＿筆 □特種個資＿＿＿＿筆
發生原因及事故摘要		
損害狀況		
個資侵害可能結果		
擬採取之因應措施		
擬採通知當事人之時間及方式		
是否於發現個資外洩後之時限內通報	初報：重大個人資料事故知悉後一小時內 □是 □否，理由：＿＿＿＿＿＿	
	續報：重大個人資料事故知悉後七十二小時內 □是 □否，理由：＿＿＿＿＿＿	
	接獲機關通報後：四十八小時內 □是 □否，理由：＿＿＿＿＿＿	

註1：各欄位資訊若尚未明確，得先填寫「不明」，並俟明確後再通報更新補充。

註2：有關通報本會方式及管道等相關資訊，另揭露於本會官網。

個資事故通報主體

- **國家發展委員會發法字第1090017079號**

➢ 法務部106年6月5日法律字第10603503230號函係就個資法第12條之釋示，雖僅就公務機關為論述，惟非公務機關亦有適用

➢ 提供網路賣家販售商品之網際網路零售服務平台業者，於個資外洩雙方責任未確定時，倘外洩之個資(例如當事人電話號碼)係平台業者及網路賣家均有蒐集者，縱未確認雙方違法責任，平台業者即應查明事實，以適當方式迅速通知當事人

個資事故之通知

- **個資法第12條**

公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人

- **通知的方式（個資法施行細則第22條第1項）**

➢ 即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之

➢ 但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之

- **通知的內容（個資法施行細則第22條第2項）**

依本法第十二條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施

事故處理之法遵義務

- 當發生疑似個資外洩時...

1 通知範圍

應通知受事故影響之當事人，如無法確定個資事故當事人範圍，則應通知所有可能受事故影響之個資當事人。

2 通知管道

原則上以便利，且可對該個資當事人發生通知效力之方式即可，如電子郵件、簡訊或電話，如以電話通知所耗費之成本或時間較高，可以電子郵件或簡訊之方式為之。

3 通知內容

（一）個資當事人個人資料被侵害之事實
（二）非公務機關已採取之因應措施（處理情形）
（三）後續供當事人查詢之專線與其他查詢管道

個資管理程序訂定之要求

- 個資檔案安全維護辦法§5

非公務機關應就下列事項，訂定**個人資料之管理程序**：

一、蒐集、處理或利用之個人資料包含**本法第六條所定特種個人資料**者，檢視其特定目的及是否符合相關法令之要件

二、檢視個人資料之蒐集、處理或利用，**是否符合免為告知之事由**，及告知之內容、方式是否合法妥適

三、檢視個人資料之蒐集、處理，是否符合本法第十九條規定，具有特定目的及法定情形；**其經當事人同意者，並應確保符合本法第七條第一項規定**

四、檢視個人資料之利用，是否符合蒐集之特定目的必要範圍；**其為特定目的外之利用者，檢視是否符合法定情形**，經當事人同意者，並應確保符合本法第七條第二項規定

五、利用個人資料為行銷，當事人表示拒絕行銷者，立即停止利用其個人資料行銷，並至少於首次行銷時，提供當事人免費表示拒絕接受行銷之方式

六、委託他人蒐集、處理或利用個人資料之全部或一部時，對受託人依本法施行細則第八條規定為**適當之監督**，並於委託契約或相關文件中，明確約定其內容

七、進行個人資料國際傳輸前，檢視是否受本會相關法令限制並遵循之

八、當事人行使本法第三條所定權利之相關事項：

（一）當事人身分之確認

（二）提供當事人行使權利之方式，並告知所需支付之費用，及應釋明之事項

（三）對當事人請求之審查方式，並遵守本法有關處理期限之規定

（四）有本法所定得拒絕當事人行使權利之事由者，其理由記載及通知當事人之方式

九、檢視個人資料於蒐集、處理或利用過程中是否正確；其有不正確或正確性有爭議者，應依本法第十一條第一項、第二項及第五項規定辦理

十、檢視所保有個人資料之特定目的是否消失，或期限是否屆滿；其特定目的消失或期限屆滿者，應依本法第十一條第三項規定辦理

十一、設置聯絡窗口供當事人申訴與諮詢

個資法規範之直接/間接告知義務

	直接蒐集時之告知義務	間接蒐集時之告知義務
法源依據	個人資料保護法§8	個人資料保護法§9
告知時機	直接蒐集	間接蒐集
告知內容	(1)蒐集機關名稱 (2)蒐集目的 (3)個資類別 (4)利用地區、期間對象與方式 (5)當事人權利行使之方式 (6)得自由提供時，不提供對當事人權益之影響 (7)間接蒐集時之資料來源	
例外規定	• 法律規定得免告知 • 係機關執行法定職務或履行法定義務所必要 • 告知將妨害法定職務執行 • 告知將妨害公共利益 • 當事人明知應告知之內容 • 蒐集非基於營利之目的且對當事人無不利影響	• 有左列情形 • 當事人自行公開或已合法公開之個資 • 不能向當事人或其法定代理人為告知 • 基於公共利益為統計或學術研究之目的而有必要等 • 大眾傳播業者基於新聞報導之公益目的而蒐集個資

告知義務例外要件試舉例

1. **法律規定得免告知**
   - 「保險法」第177條之1第3項，保險業為執行核保或理賠作業需要，處理、利用依法所蒐集保險契約受益人之姓名、出生年月日、國民身分證統一編號及聯絡方式，得免為個人資料保護法第九條第一項之告知。
2. **係機關執行法定職務或履行法定義務所必要**
   - 稅務機關蒐集納稅人之所得資料，即屬公務機關執行法定職務所必要
3. **告知將妨害法定職務執行**
   - 法院執行扣押個人的財產，若將蒐集個人資料的狀況告知，該個人可能因而脫產，影響扣押的執行
4. **告知將妨害公共利益**
   - 線人資料來源
5. **當事人明知應告知之內容**
   - 個人的郵局金融卡遺失，向郵局申辦新的金融卡，其提供個人資料時，已知應告知的事項，所以郵局不需要再為告知
6. **蒐集非基於營利之目的且對當事人無不利影響**
   - 為提供員工免費通勤接駁車

蒐集資料變更之告知義務

問題：業者蒐集資料變更，應如何踐行告知義務？

國家發展委員會民國 107 年 11 月 21 日發法字第 1072002136號函

業者倘因服務延伸致需衍生蒐集新的個人資料，於**蒐集**該次變更項目之個人資料**前**，**不論特定目的是否改變，皆須依個資法第8條第1項規定履行告知義務**。惟業者對於過去已告知當事人之相同事項，得斟酌個案情形，依據個資法施行細則第16條之規定，運用各種技術以簡化或便利之方式通知當事人(例如：透過超連結之方式，顯示先前已告知之相同內容，由當事人自行點選檢視)

健身房入會時之個資告知事項，並未提及「照片」及「生物特徵」之蒐集，是否有違反個資法之虞？

- 健身會員合約書，僅記載「會員收到會員卡後，同意讓櫃臺服務人員照相存檔，以便於每次進入會所時核對身份。」故除「照片」外，應依個資法**第8條第1項規定完整向當事人告知其他蒐集之個人資料類別**（如生物特徵資料）
- 健身工廠與會員間訂立契約，基於會員服務及會所管理之特定目的，得依個資法第19條第1項第2款及第20條第1項本文規定，於**履行契約必要範圍內**蒐集、處理及利用會員之個人資料
- 倘經教育部體育署審認蒐集會員臉部辨識資料**非屬履行契約所必要**，則得另**基於當事人同意**，依個資法第19條第1項第5款規定蒐集其臉部辨識資料，且應依個資法第8條規定踐行告知義務。至於會員續約時倘不同意蒐集其臉部辨識資料，則雙方是否締約應回歸契約自由原則

何謂當事人之「同意」？

- 個資法第7條第1至3項
  - 第十五條第二款及第十九條第一項第五款所稱同意，指當事人經蒐集者**告知本法所定應告知事項後**，所為**允許**之意思表示
  - 第十六條第七款、第二十條第一項第六款所稱同意，指當事人經蒐集者**明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響**後，**單獨所為**之意思表示
  - 公務機關或非公務機關明確告知當事人第八條第一項各款應告知事項時，當事人如**未表示拒絕**，並**已提供其個人資料**者，推定當事人已依第十五條第二款、第十九條第一項第五款之規定表示同意
- 甲公司於協助小明宅配所購電腦之際，告知甲公司蒐集小明個資之目的（包括宅配、行銷等）、範圍、當事人權利行使方式及其他應告知內容
  - ✓ 小明表示OK
  - ✓ 小明不置可否
  - ✓ 小明「喔」了一聲
  - ✓ 小明詢問接到行銷電話的頻率，聽到甲公司的回答後，說了一句「還好不會太常打」
  - ✓ 小明自行拿走甲公司放在櫃臺上，包裝上清楚印有「電話行銷客戶贈品」之刮鬍刀一支
- 若小明為未成年人？

書面同意vs電子方式？

- **法務部102年03月21日法律字第10203502480號函**

應考人於進行國家考試網路報名系統進行報名前，均經告知並需填具同意書，始得進行網路報名，**則該同意書雖係以電子方式為之，倘足以確認當事人之意思表示，並有可為證明之方式（電子簽章法第4條第2項規定參照）**，即具有本法第7條第2項**「書面同意」之效力**（經濟部100年10月27日經商字第10000663080號函參照），從而戶役政機關及各級學校將應考人個人資料提供貴部查驗，即符合本法第16條第7款、第20條第1項第6款「經當事人書面同意」之情形，而得合法為個人資料之特定目的外利用

推定同意？

問題：預設同意是否屬於推定當事人同意？

- **國家發展委員會民國 107 年 11 月 21 日發法字第1072002136號函**

➢ 按個資法第7條第3項規定「公務機關或非公務機關明確告知當事人第8條第1項各款應告知事項時，當事人如未表示拒絕，並已提供其個人資料者，推定當事人已依第15條第2款、第19條第1項第5款之規定表示同意」。因此業者如欲透過「推定同意」之方式取得個人資料，除**應盡告知義務且明確告知**外，尚須符合**「當事人未表示拒絕」及「當事人已提供其個人資料」兩項要件**，始得為之。

➢ 本件若欲符合推定同意要件之「當事人已提供其個人資料」，應係指**當事人有自行提供個人資料之積極行為**(例如：自主開啟藍芽設定並選擇同步資料，並將資料傳送予業者)；**倘業者預設自動上傳資料之功能，在當事人未有任何積極行為之情形下即取得個人資料，則縱使當事人未表示拒絕，仍不得視為當事人已提供其個人資料，因此應不符合**

同意之方式及內涵-兒童個資？

問題：蒐集兒童個資時的告知與同意取得？

- **國家發展委員會民國 108 年 03 月 12 日發法字第1082000384號函**

教材業者欲基於當事人同意，蒐集未成年學童之個人資料，除應注意**業者以贈品誘使學童提供個人資料，是否已違反個資法第5條之誠實信用原則**外，業者另**應踐行個資法第8條第1項相關法定應告知事項**，徵諸上開立法理由，應使當事人得以充分瞭解後審慎為之，是業者之告知方式**應符合學童之年齡、生活經驗及理解能力，以容易理解、清楚簡單之語言或文字為之，並使該學童得以充分瞭解其個人資料之後續利用**。倘教材業者未完整踐行告知，或其告知對象無法充分瞭解其個人資料之後續利用，則未能符合個資法第7條第1項之規定。另蒐集者就當事人同意合法要件之事實，應負舉證責任（同法第7條第4項規定參照），併予敘明

未成年人同意權之行使

戶政事務所使用「輔助人員辨識確認系統」拍攝14歲以上之未成年人臉部影像所涉下稱個資法問題（國家發展委員會發法字第1100005839號）

- 戶政事務所蒐集臉部影像並透過「輔助人員辨識確認系統」辨識當事人身分，鑒於「臉部影像」具有人各不同、終身不變之生物特徵特質，屬具備高度人別辨識之個人資料，除應尊重當事人權益，注意是否為辨識當事人身分之最小侵害方式等；並應注意**以符合當事人年齡、生活經驗及理解能力，踐行法定應告知事項**
- 以同意蒐集14歲以上之未成年人臉部影像，因個資法就未成年人權利行使之年齡並無特別規定，故未成年人同意權之行使，**應回歸民法有關行為能力之一般性規定**
  - 未滿七歲之未成年人，無行為能力。 滿七歲以上之未成年人，有限制行為能力。限制行為能力人為意思表示及受意思表示，應得法定代理人之允許。但純獲法律上利益，或依其年齡及身份、日常生活所必需者，不在此限

GDPR規範下之當事人同意

核心內容	說明
定義	◆ 資料當事人基於其自由意志、具體、知情且不含糊，透過積極明確之行動聲明表示同意處理與其有關個人資料之意思表示 ◆ 取得同意做為處理有關其特種個資時，更強調需經得當事人「明確同意」（explicit consent）
重要性	◆ 透過當事人同意取得，可以多元化使用個資進行處理或分析 ◆ 可突破部份法規上的使用限制，例如特種個資合法處理、資料境外傳輸、自動化剖析合法化
當事人同意強化	◆ 需要當事人基於自由意志給予、出於真意的選擇及控制 ◆ 同意必須基於特定目的下清楚且具體描述給予 ◆ 同意需獲通知後給予 ◆ 同意必須經明確表示 ◆ 同意必須是一種經聲明或確定行動的行為 ◆ 同意請求必須與其他條件或條款明顯區隔 ◆ 不得將同意之取得做為是否提供服務之先決條件 ◆ 同意請求必須採用清晰、明瞭且易懂的語言，並易於取得 ◆ 不定期確認組織同意條款內容，必要或有變動時應更新，確保取得同意的有效性 ◆ 對當事人所為同意之意思表示留下證明

抖音Tiktok違反GDPR遭罰75萬歐元

● 抖音TIKTOK無完備個資告知義務

使用者創設抖音TIKTOK帳戶時，他們必須同意抖音的隱私權條款，然而荷蘭個資主管機關發現在2018年5月到2020年7月期間，這些隱私權條款僅有英文版本
此種措施違反了GDPR第12條第1項關於個資告知的透明性義務

GDPR第12條第1項規範控制者應採取合理的措施提供所有與個人資料處理相關的資料，並應該要具體、透明並且可取得的形式、且使用清晰平易近人的語言，特別是蒐集個資對象包含兒童時。並且在依據GDPR發布關於透明性Guidlines第14點中，要求為了要使18歲以下之人以及孩童可以知道他們具有哪些權利以及哪些個資提供，必須使用讓兒童可以產生共鳴的詞彙

因此，抖音TIKTOK要清楚的辨認其潛在觀眾的特質、年紀以及是否有特殊需求。因此抖音TIKTOK有義務去為了青少年、甚至是兒童撰寫他們可理解的隱私條款。暫且不論是否要使用白話文程度應到何種程度，但採用僅有英文的版本就是違反了個資蒐集處理使用的通知義務。荷蘭個資主管機關對抖音TIKTOK處罰了75萬歐元（約2500萬台幣）

撤回同意

- **法務部 106年11月10日法律字第10603512680號函**

按個人資料保護法（下稱個資法）第11條第3項規定：「個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。」準此，倘業者基於當事人同意合法蒐集、處理之個人資料（個資法第19條第1項第5款參照），而當事人事後撤回其同意，則**自其撤回時起**，如蒐集個人資料之特定目的或要件已不存在，除有上開個資法第11條第3項但書規定之情形（個資法施行細則第21條規定參照）外，**業者應主動或依當事人之請求，刪除、停止處理或利用該等個人資料**，合先敘明

個人資料紀錄、證據保存機制之建立

- 個資檔案安全維護辦法§6

非公務機關應就下列事項，訂定相關**紀錄、證據保存機制**：

一、因執行本計畫及處理方法所定各種個人資料保護機制、程序及措施，所記錄之**個人資料使用情況、軌跡資料及相關證據**

二、依本法第十一條第三項規定刪除、停止處理或利用所保有之個人資料後留存之下列紀錄：

（一）刪除、停止處理或利用之方法、時間

（二）將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉原因、對象、方法、時間，及該對象蒐集、處理或利用之合法依據

個人資料作業流程建置前–初步檢視

- **公司營業項目**
  - 營業項目所跨及之領域
  - 公司性質可能牽涉的主管機關及法規
- **公司作業流程**
  - 公司現有作業流程的初步判斷
- **公司重要業務**
  - 營運、獲利、客戶……等，公司重點業務

個資作業流程繪製原則

- **考量**：避免部門負擔，達成部門個資管理目的
- **方式：作業流程 + 標註個資事項**
  - 建立/擇取**現行作業流程**

  - 辨識並標註涉及**個資蒐集、處理或利用之節點**

  - 辨識並標註涉及**個資管理應辦事項之節點**

個資作業流程

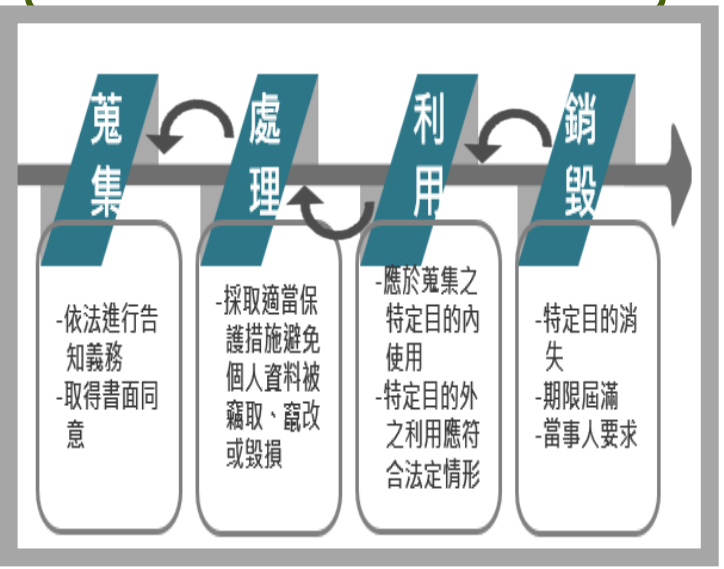
例如：應使用個資同意書、
應於個資管理系統盤點等等

- **注意**：除了**部門內單位或部門間**流動，也要納入**外部主體（尤其委外廠商）間**之流動

涉及個人資料之檔案均應納入盤點

個資法規範的範圍

直接及間接識別之個人資料



整個個資生命週期(各階段)都應具備適法性

如果不盤點，則無目的、保存期限等相關資訊，可以據以檢視、管理那些個資已**不具適法性**，且亦難以確保有無**情事變更**的可能性，如：

①特定目的已消失(蒐集目的為連繫用，但後續已不需再連繫)

②保存期限已屆滿(保存期限為5年，但早已超過6年)

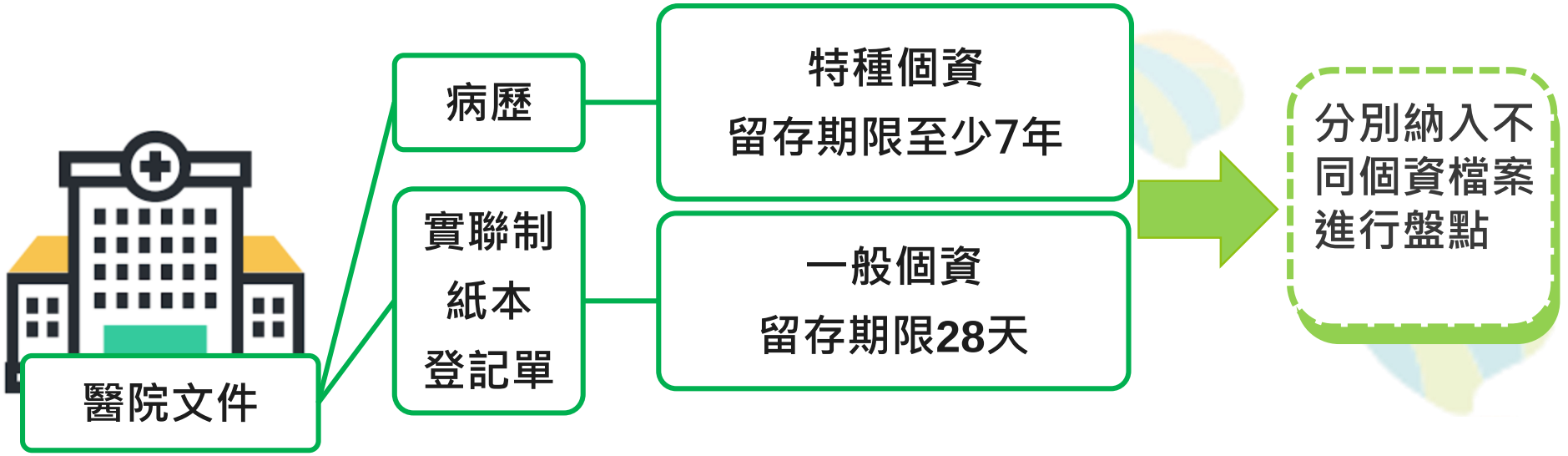
③是否有目的外利用(原目的為市調，後竟用於行銷)

④留存個資之目的主要係提供國稅局查核之用，但仍有調查局、法院調閱查案的可能性

因此涉及個人資料之檔案均應納入盤點，透過個資盤點，才能有目的、保存期限等相關完整資訊，後續也才能據以**定期檢視**個資生命週期各階段的適法性。若在檢視過程中發覺欠缺適法性，應立即刪除、停止處理或利用該等個資

思考-實聯制之個資檔案進行盤點

- 需將特定目的、風險值相同或相近之個資分類，納入同一個資檔案進行盤點，並採行適當安全維護措施
- 如：將100份病歷以及50份實聯制紙本登記單**分別**納入**不同**的個資檔案進行盤點，個資總筆數則分別為100筆及50筆(從業務流的角度出發，而將一份表單上所載的所有資料定義為一筆個資)



涉及個資之檔案應由何部門盤點(1/3)

Q

個資檔案之正本係從各業務部門蒐集、傳遞而來，電子檔由業務部門上傳於系統，正本則由幕僚部門保管、利用，應由何部門盤點？

A

視實際上由那一個部門進行目的內之處理與利用定之，因實際處理或利用之部門**最瞭解特定目的、情形、保存期限，以及實際存放位置**等資訊，由其負責盤點最有利於達成盤點之目的

涉及個資之檔案應由何部門盤點(2/3)

- 以簽到表為例，業務部門出於**確認出席人員**之目的而蒐集個資，因此最瞭解特定目的及情形，由業務部門進行盤點才能落實個資盤點之目的。但因簽到表正本後續將傳遞到會計部門留存(處理)，凡涉及個人資料之檔案均應納入盤點，由於會計部門持有個資檔案之正本，因此亦應針對簽到表進行盤點，惟此時之特地目的則有所不同(**稅務佐證**目的)

特定目的：確認出席人員
存放位置：電子檔存特定系統
紙本傳遞會計處
保存期限：計畫結案後

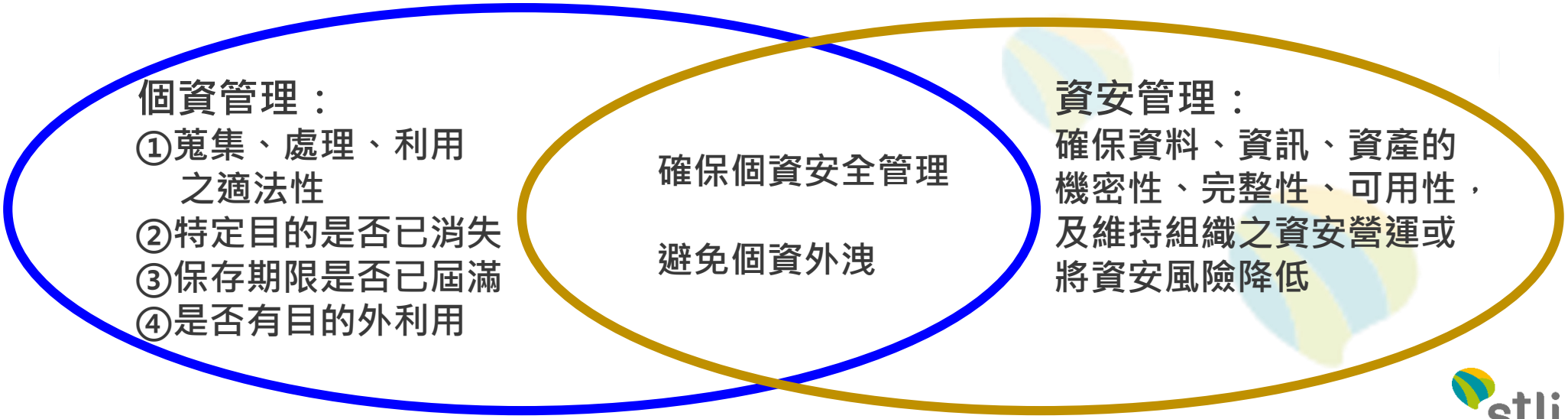
蒐集主體：公司
蒐集方式：直接蒐集
當 事 人：含一般人士
是否委外：否
個資類別：姓名、職稱
檔案形式：紙本、電子檔
告知義務：已履行

特定目的：稅務
存放位置：電子檔存財會系統
紙本存放倉儲
保存期限：10年

涉及個資之檔案應由何部門盤點(3/3)

Q 是否統由資訊部門進行系統整體盤點、風險評估即足以說明個資之風險控制？

A 個資管理**不完全等同**於資安管理，兩者之保護需求有所不同。例如：部門執行二年期計畫而蒐集個資，存放於資訊部門所建置之系統，並進行數據分析。資訊部門負責確保系統內資料的機密性、完整性、可用性，但對於個資檔案之特定目的、情形、類別、數量、形式、保存期限，以及實際處理或利用等相關資訊並不明瞭，若由資訊部門為整體盤點，並無法達到盤點及管理之目的及實益



個人資料流程清點

誰會經手這些資料？
部門/外部單位？

為什麼需要這些資料？
對這些資料做了什麼事？

什麼時候取得/使用資料？
資料會保存多久？

資料保存在哪裡？
什麼介質？

蒐集哪些資料？

Q：會計憑證應如何進行盤點

Q 今天龍年大吉公司邀請李老師來公司上個資法的課程，法務要求李老師提供領據，人資處在開課前，亦要求學員記得要在簽到表上簽名，請問應該如何進行個資盤點？

簽到表		
編號	部門	簽名

收　　據

茲收到 (單位名稱) 辦理課程：

講師費計新臺幣　元正

日期：　　時間：　　聘別：□外聘 □內聘

姓名:　　簽名或蓋章(私章)

專業背景或簡歷：

身分證字號：

戶籍地址：

聯絡電話：

中 華 民 國 113 年　月　日

思考-會計憑證應如何進行盤點(1/3)

Q 紙本傳票、系統保管裡的個資是否需要逐筆盤點？

A 由於個資的蒐集目的、情形、類別、保存期限、敏感程度、風險評價值均**不盡相同**，若將所有個資概括混入同一個資檔案盤點，則**無法辨別**出個資檔案中各資料間的**差異**及相關資訊，並施以不同的管理措施

收據
①目的：稅務
②個資類別較多
③涉及敏感程度較高之身分證統一編號
④保存年限較長

簽到表
①目的：確認出席人員
②個資類別較少
③個資敏感程度較底
④保存年限較短

思考-會計憑證應如何進行盤點(2/3)

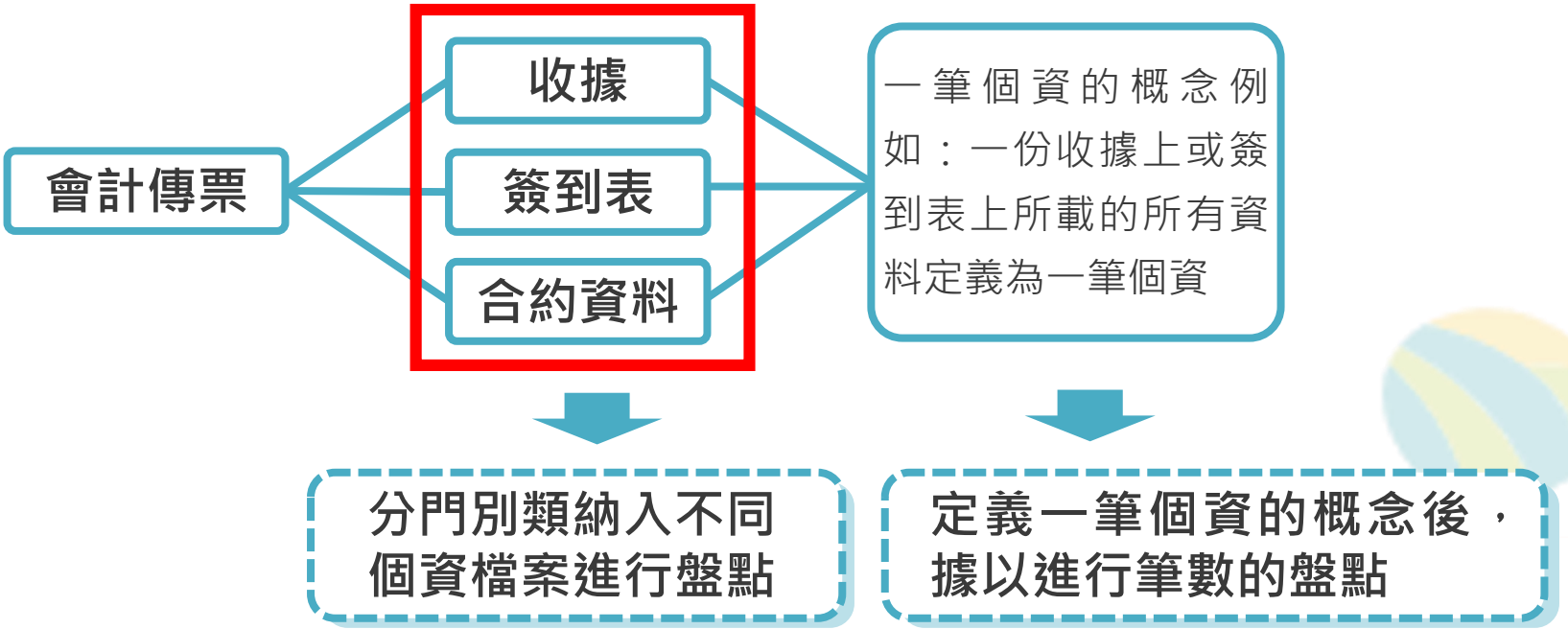
- 以組織留存個資之可能情形為例：

收據	簽到表	連繫單	其他個資
目的：稅務 情形：法律規定 類別：姓名、地址、身分證字號。(另有可能蒐集電話號碼) 形式：紙本 期限：5年	目的：確認出席人員 情形：當事人同意 類別：姓名、職稱 形式：紙本 期限：計畫結案	目的：連繫 情形：取自一般可得來源 類別：姓名、職稱、電話號碼 形式：電子檔 期限：1年or後續不再連繫	目的：_____ 情形：_____ 類別：_____ 形式：_____ 期限：_____

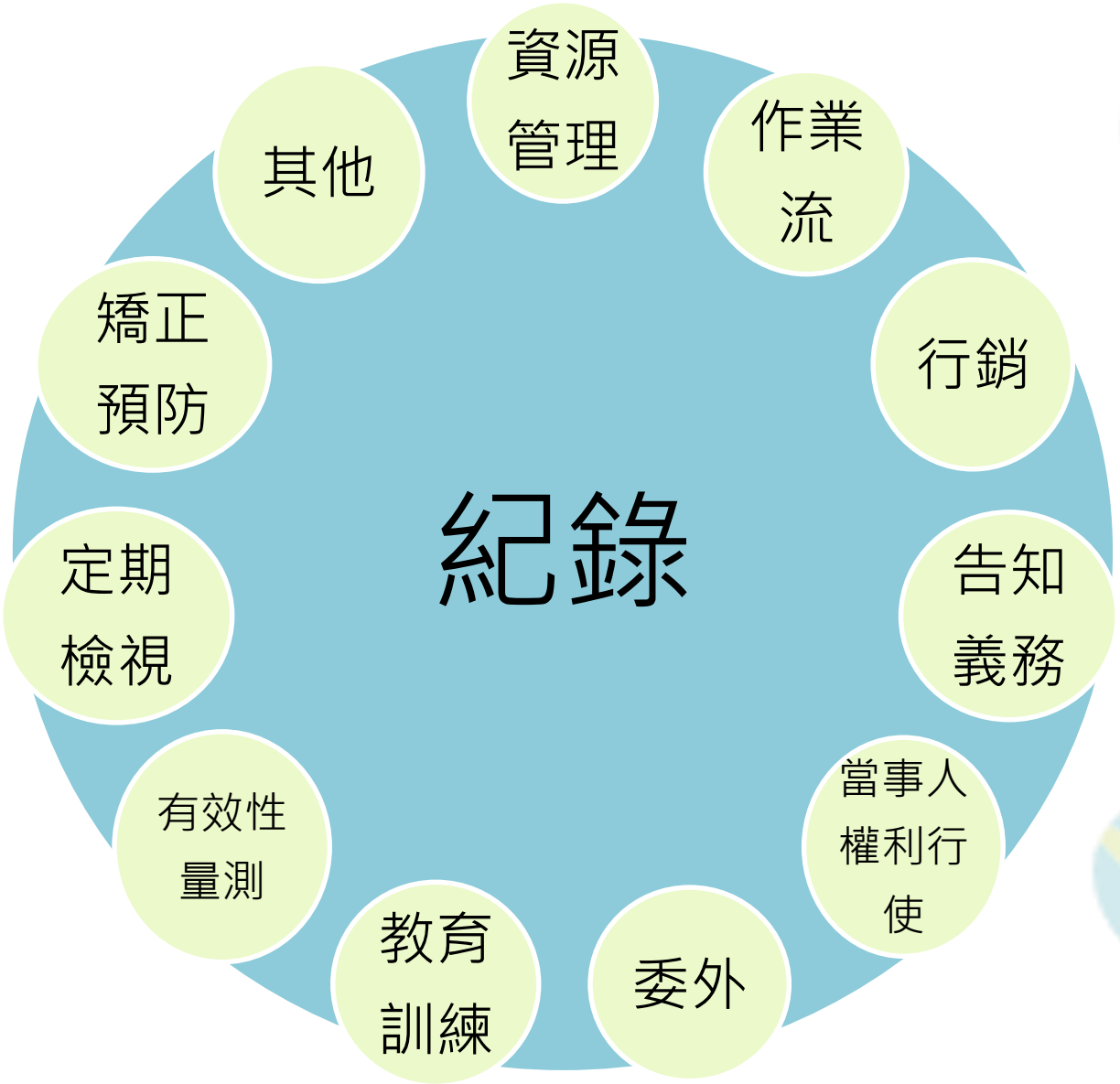
若將所有個資概括混入同一個資檔案盤點，並以**一箱或一批**個資進行盤點，則完全無法辨別各資料間的差異及相關資訊，不僅難以達成個資盤點的目的，更有可能因而招致稽核人員的關切

思考-會計憑證應如何進行盤點(3/3)

- 由於**紙本傳票**及**財會系統**混雜許多不同的個資，若僅以之作為盤點之標的，難以實現盤點及個資管理之目的
- 較適宜之作法可將紙本傳票所附稅務、簽到表、合約等資料，以及財會系統裡之資料分門別類，將特定目的、風險值相同或相近之資料，納入同一個資檔案進行盤點，並從自身業務流的角度出發，定義一筆個資



文件與紀錄管理



記錄管理重點

結合內部管理

因應法規要求

協助訴訟舉證

管理重點

使用紀錄、軌跡資料及證據保存可作為內部安全管理措施之一環，如軌跡資料包含相關log紀錄，可判別資料存取人員、時間、設備等，搭配內部控制作為或規範，倘發生有異常狀況，即可適時處理

配合個資法第7條修正，蒐集者對當事人同意之事實負有舉證責任，如有相關使用紀錄、軌跡資料及證據保存，亦可協助訴訟程序之舉證

個資保護違法責任總覽

民事責任：§28~§40

刑事責任：§41~§46

行政責任：§25、§47~§50

行政檢查配合義務(1/3)

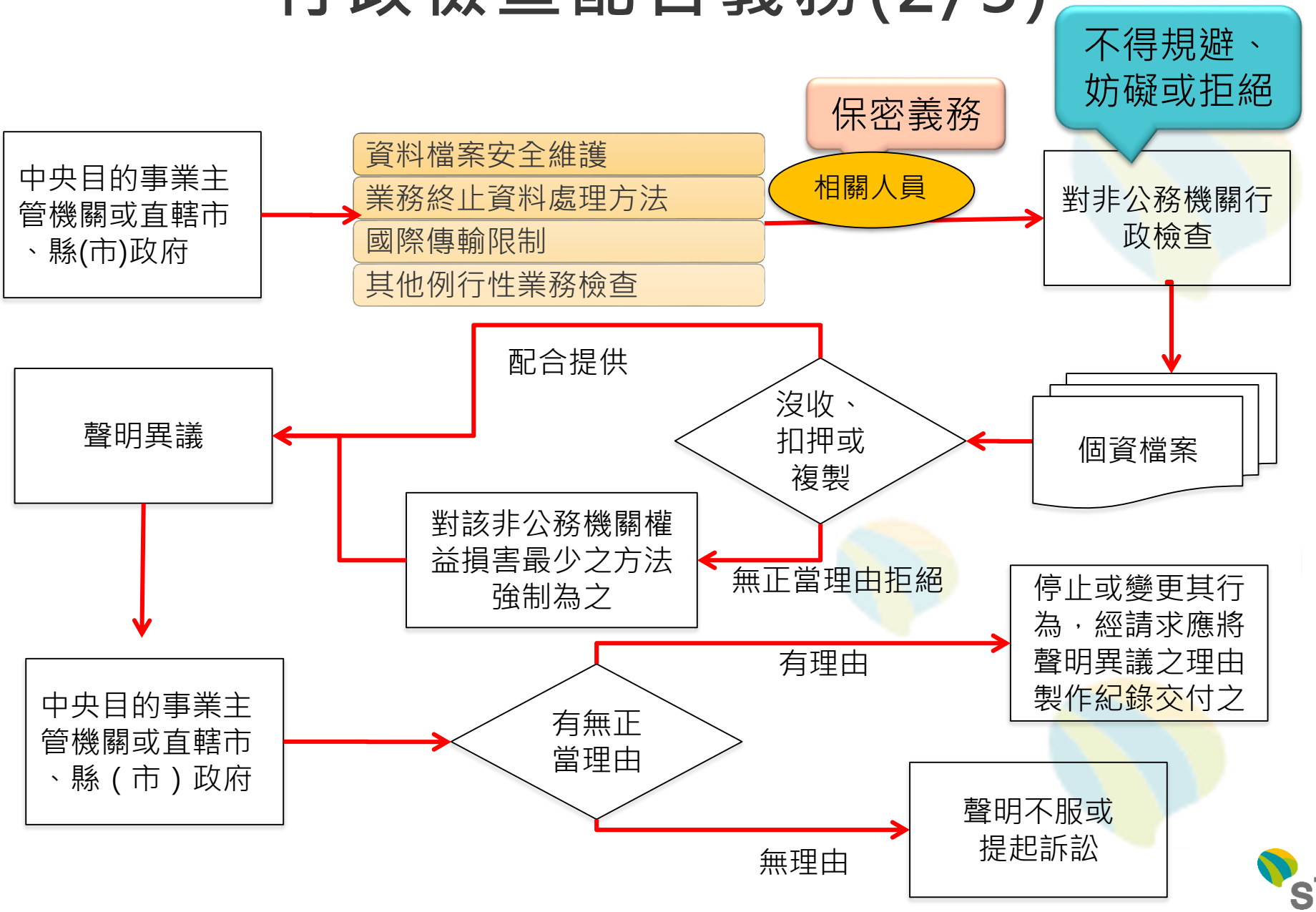
個資法第22條

- 中央目的事業主管機關為執行資料檔案安全維護、業務終止資料處理方法、國際傳輸限制或其他例行性業務檢查而認有必要或有違反本法規定之虞時，得派員攜帶執行職務證明文件，進入檢查，並得命相關人員為**必要之說明、配合措施或提供相關證明資料**
- 中央目的事業主管機關或直轄市、縣（市）政府為前項檢查時，對於得沒入或可為證據之個人資料或其檔案，得**扣留或複製**之。對於應扣留或複製之物，得要求其所有人、持有人或保管人提出或交付；無正當理由拒絕提出、交付或抗拒扣留或複製者，得採取對該非公務機關權益損害最少之方法強制為之
- 目的事業主管機關或直轄市、縣（市）政府為第一項檢查時，得率同資訊、電信或法律等專業人員共同為之
- 對於第一項及第二項之進入、檢查或處分，非公務機關及其相關人員**不得規避、妨礙或拒絕**
- 參與檢查之人員，因檢查而知悉他人資料者，**負保密義務**

個資法第49條

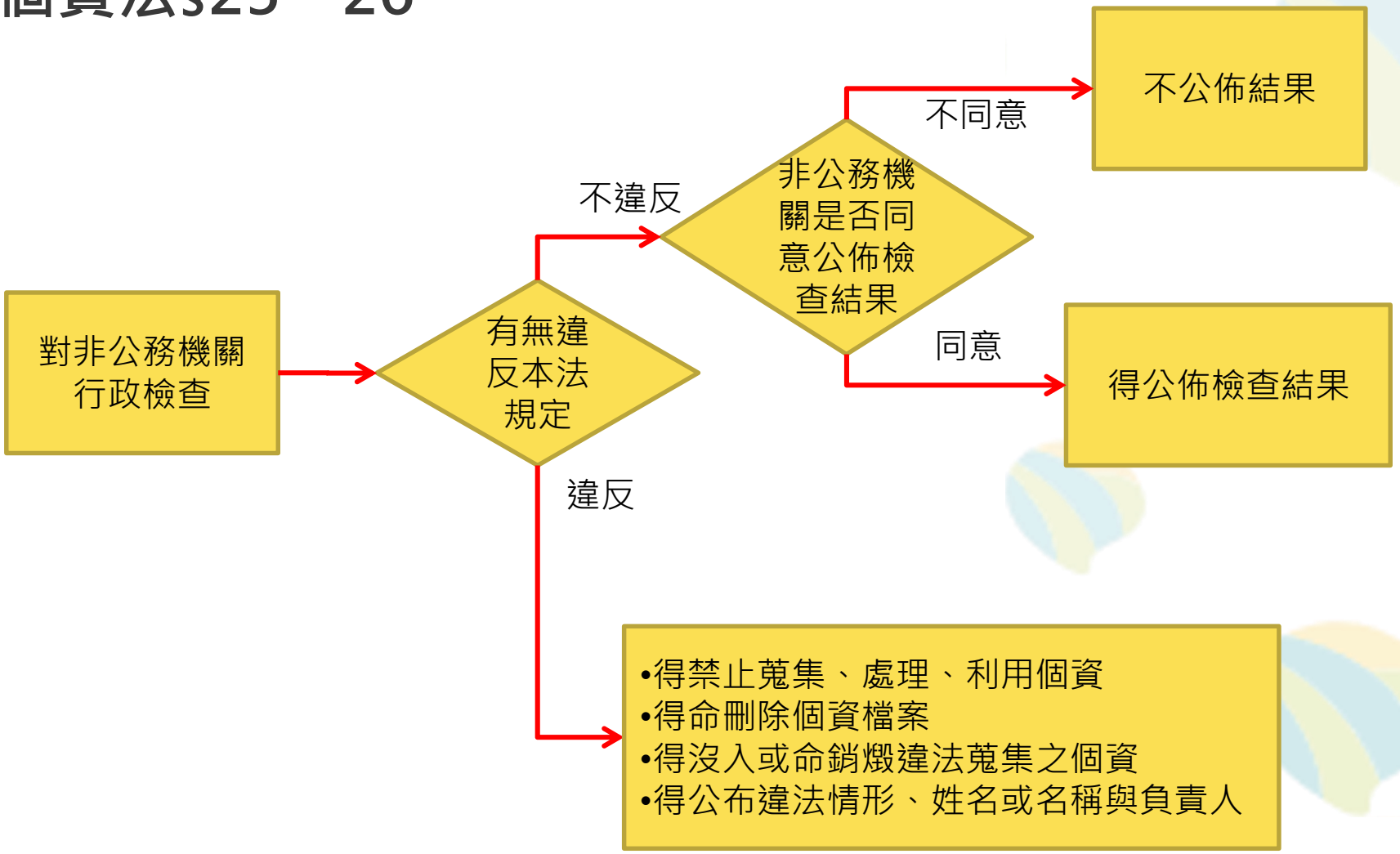
非公務機關無正當理由違反第二十二條第四項規定者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣**二萬元以上二十萬元**以下罰鍰

行政檢查配合義務(2/3)



行政檢查配合義務(3/3)

- 個資法§25、26



違法責任種類及其內涵

刑事 –
有期徒刑、罰金

處**五年以下有期徒刑**，**得併科新臺幣一百萬元以下罰金**

§41
違法行為態樣
意圖為自己或第三人不法之利益或損害他人之利益，而違反以下規定：
第6條第1項
（違法蒐集、處理、利用特種資料）
第19條
（無特定目的或特定情況而蒐集、處理資料）
第20條第1項
（利用資料逾越特定目的）
第21條
（違反限制國際傳輸之命令或處分）

民事 –
侵權行為損害賠償

每一事件酌定：
新台幣500 - 20,000元
總額：**新台幣2億元**

行政 – 罰鍰等

處新臺幣2-200萬元以下罰鍰，並令其限期改正，屆期未改正者，按次處新臺幣15-1,500萬元以下罰鍰

違法責任：刑事責任(1/2)

罪名	法條 §41~46
非法蒐集、處理或利用個人資料罪	§41、§43、§44
非法妨害個人資料檔案正確性罪	§42、§43、§44
其他條文之追訴條件	1. §46：犯本章之罪，其他法律有較重處罰規定者，從其規定 2. §45本文：本章之罪，須告訴乃論 3. §45但書：但犯第四十一條之罪者，或對公務機關犯第四十二條之罪者，不在此限

違法責任：刑事責任(2/2)

條次	行為種類	處罰結果
§41	**意圖**為自己或第三人不法之利益或損害他人之利益，而違反以下規定： 違反第六條第一項（違法蒐集、處理、利用特種資料） 違反第十九條（無特定目的或特定情況而蒐集、處理資料） 違反第二十條第一項（利用資料逾越特定目的） 違反第二十一條（違反限制國際傳輸之命令或處分）	處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金
§42	**意圖**為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人	處五年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金

刑事責任案例分享(1/2)

- 個資法第41條所稱「利益」應限於財產上之利益；至同條所稱「損害他人之利益」中之「利益」，則不限於財產上之利益（最高法院109年度台上大字第1869號裁定意旨參照）

- 鄰居因故發生糾紛，當事人將翻攝之調閱監視器畫面，連同和解過程取得之姓名、年齡、特徵、犯罪前科、財務狀況等個資，上傳Youtube等網站。於無個資法第20條第1項但書所定之例外事由下，不得逾越原始和解之目的，量處有期徒刑3個月，並得易科罰金（107,上訴,313）

*個資法第41條：意圖為自己或第三人不法之利益或損害他人之利益，而違反第六條第一項、第十五條、第十六條、第十九條、第二十條第一項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分，足生損害於他人者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金

刑事責任案例分享(2/2)

- 被告於民國103年間非法取得安裝有大量全國自然人姓名、出生年月日、國民身分證統一編號、聯絡方式及任職單位等個人資料之「people」搜尋系統之筆記型電腦，再提供予付費購買之仲介業者，並以查詢每5筆個人資料，收費新臺幣1,350元至1,500元之交易模式，犯個資法第四十一條非法利用個人資料罪，處有期徒刑6月，得易科罰金（111年度原訴字第69號）
- 被告於110年4月26日先後至台新銀行仁愛分行及忠孝分行丟撒傳單之行為，犯個人資料保護法第四十一條之非公務機關非法利用個人資料罪， 處有期徒刑3月，得易科罰金（111 ,簡, 1736）
- 被告與原告同為藝人，於臉書直播時，被告念出原告電話前四碼，搭配與原告門號末6碼相同數字之色號卡圖片，使不特定人透過文章結合，知悉原告門號，犯個人資料保護法第四十一條之非公務機關未於蒐集特定目的必要範圍內利用個人資料罪，處有期徒刑肆月，如易科罰金，以新臺幣壹仟元折算壹日（111年度訴字第1024號）

*個資法第41條：意圖為自己或第三人不法之利益或損害他人之利益，而違反第六條第一項、第十五條、第十六條、第十九條、第二十條第一項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分，足生損害於他人者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金

違法責任：民事責任

賠償原因	違反本法規定，致個人資料遭不法蒐集、處理利用或其他侵害當事人權利
抗辯理由	證明其無故意或過失。
賠償金額	個人：新台幣500元～20,000元 總額：新台幣200,000,000元
其他賠償	名譽被侵害者，並得請求為回復名譽之適當處分。
請求權時效	自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅；自損害發生時起，逾五年者，亦同
訴訟方式	有團體訴訟之規定（20人以上）

團體訴訟

雄獅個資外洩團體訴訟進度表

日期	進度	備註
106年05月23日	報載	雄獅旅遊於106年5月23日發布聲明揭露，公司內部員工電腦作業系統遭駭客入侵，造成36萬筆消費者個資外洩，包括姓名、聯絡電話和購買商品資料等。
106年9月6日	協調會	
107年03月1日	至臺灣士林地方法院遞交民事起訴狀	當日舉辦記者會。
107年5月10日	地方法院言詞辯論	一審開庭
107年11月29日	地方法院言詞辯論	一審開庭
108年1月17日	地方法院言詞辯論	一審開庭
108年3月28日	地方法院言詞辯論	一審開庭
108年5月23日	地方法院言詞辯論	一審開庭
108年9月19日	地方法院言詞辯論	一審開庭
108年10月31日	地方法院一審宣判	
108年11月21日	提起上訴	
109年3月25日	高等法院準備程序	二審開庭
109年5月8日	高等法院準備程序	二審開庭
109年7月1日	高等法院準備程序	二審開庭
109年7月7日	高等法院調解程序	二審開庭
雄獅團訟案在109年7月7日於臺灣高等法院民事庭成立調解。 1.於確認收到賠償金後，於8月中旬寄出消費者領取通知。 2.9月中旬消費者皆已申請領取，9月底核發完畢。		

和雲 Irent 個資外洩風險訴訟可能走向樹狀圖

臉書 iRent 個資案團體訴訟團 2023.02.16

民事責任案例分享(1/2)

- 某賣場於會員表示拒絕接受行銷簡訊後仍持續寄送訊息，遭判賠1.6萬元（每封1000元）及1萬元慰撫金，共計2.6萬元（103,湖小,537）
- 民眾於某網購平台個資外洩，遭取消分期付款詐騙，民眾依照個資法第29條向某網購平台請求損害賠償。並主張該平台未依照個資法第12條及個資法施行細則第22條告知其「資料被侵害之事實」及「採取之因應措施」，平台顯然疏於個資安全防護責任，遭判賠2萬元（108,北小,718）

民事責任案例分享(2/2)

- 臺灣高等法院112 年度上字第 656號民事判決

被上訴人不法侵害上訴人隱私權、個資自主權，致上訴人系爭個資為詐騙集團不法利用，依個資法第29條、第28條第2、3項之規定，被上訴人XX溫泉公司及XX網路科技公司遭判賠**應分別給付上訴人新臺幣貳萬元慰撫金：**

- 個人資料保護法第 27 條規定，非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。同法第 29 條規定，若非公務機關違反規定，致個人資料遭不法侵害，負損害賠償責任。但能證明其無故意或過失者，不在此限。**科技公司保有個資而發生個資遭不法侵害**，採**過失推定原則**，即由**科技公司舉證證明其無故意或過失，才能免責**

- 又消費者的個資是由科技公司存放於該系統中，消費者無法自行使用、管理，依**民事訴訟法第 277 條但書規定應輕減消費者的舉證責任**。又主管機關的調查程序與訴訟事件程序不同，且其認定並無拘束法院的效力，故**溫泉公司無法證明**消費者個資遭竊外洩前，已就科技公司管理維護訂購系統，**為適當監督的行為**，**科技公司也無法證明**網路訂購系統對於消費者的個資，**已採行適當安全措施的責任**，因而溫泉公司及科技公司**均需對消費者個資的外洩負損害賠償責任**

違法責任：行政責任(1/2)

條次	違反行為種類	處罰結果
§47	第六條第一項（違法蒐集、處理、利用特種資料） 第十九條（無特定目的或特定情況而蒐集、處理資料） 第二十條第一項（利用資料逾越特定目的） 第二十一條（違反限制國際傳輸之命令或處分）	處新臺幣五萬元以上五十萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之
§48	違反第八條或第九條規定。（違反告知義務） 違反第十條、第十一條、第十二條或第十三條規定。（妨礙當事人行使權利） 違反第二十條第二項或第三項規定。（違反拒絕行銷之規定）	限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰
	違反第二十七條第一項（適當安全措施）或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。	處新臺幣二萬元以上二百萬元以下罰鍰，並令其限期改正，屆期未改正者，按次處新臺幣十五萬元以上一千五百萬元以下罰鍰

違法責任：行政責任(2/2)

條次	違反行為種類	處罰結果
§49	無正當理由違反第二十二條第四項規定者（妨礙行政檢查）	處新臺幣二萬元以上二十萬元以下罰鍰
§50	非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條規定受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰	受同一額度罰鍰之處罰 ->**兩罰主義**
§25	上述各項違法行為	禁止蒐集、處理或利用個人資料 命令刪除經處理之個人資料檔案 沒入或命銷燬違法蒐集之個人資料 公布非公務機關之違法情形，及其姓名或名稱與負責人

違法行銷之行政責任

- 某健身房利用三年前的會員資料（會員已到期），不停以電話行銷其所販售之服務，民眾要求停止利用其個資行銷未果向主管機關檢舉。試問該健身房違法行銷之行政責任為何？
- 法律字第10303501900號函釋
  - 非公務機關利用個人資料從事商品行銷時，無論係特定目的內或特定目的外之利用，本法賦予當事人拒絕接受行銷之權利，以保障其免受行銷之打擾；當事人表達拒絕接受行銷之意思表示時，非公務機關應即停止再利用其個人資料進行行銷，爾後亦不得再利用其個人資料進行行銷。主管機關應命限期改正，屆期未改正者，按次處新臺幣2萬元以上20萬元以下罰鍰（本法第48條第3款參照）

行政檢查-受稽查方之協力義務

- 消費者向主管機關檢舉某電腦公司違法個資法蒐用其個資，主管機關是否能強制電腦公司提供相關資料並說明之？
- **法律字第10703511710號函釋**

  政府機關如為調查公司涉及違反個人資料保護法案件，得依行政程序法第40條規定要求公司提供必要之文書、資料或物品，若其拒絕提供，而機關認有必要或有違反個資法規定之虞，個資法第22條第1項及第2項規定進入檢查並為相關保存證據之處分，如該公司無正當理由規避、妨礙或拒絕者，得裁處新臺幣2萬元以上20萬元以下罰鍰（個資法第22條第4項及第49條參照）

行政責任裁罰案例(1/4)

首頁 經濟VIP 經濟彭博 即時 要聞 產業 證券 行情 國際 兩岸 金融 期貨

訂閱

14:39 日圓走勢大翻轉 由貶破160大關轉為暴衝 出現干預跡象

經濟日報 > 要聞 > 政經焦點

數位部開罰！個資外洩未改善 蝦皮被罰20萬、誠品10萬

蝦皮。記者黃筱晴／攝影

櫃買中心表示，連鎖藥妝通路諾貝兒（丁丁連鎖藥妝）9月發生客戶資料外洩情事，卻未依照規定發布重訊公告，裁處15萬違約金。（示意圖，諾貝兒提供）

〔記者歐宇祥／台北報導〕櫃買中心今日表示，連鎖藥妝通路諾貝兒（丁丁連鎖藥妝）（6844）9月發生客戶資料外洩情事，卻未依照規定發布重訊公告，裁處15萬違約金。

櫃買中心說明，諾貝兒在9月14日查知客戶資料疑有外洩之情事，但未依規定於期限內發布重大訊息，核有違反興櫃股票審查準則第34條規定之情事，櫃買中心依興櫃股票審查準則第62條規定，對該公司處以違約金15萬元。

行政責任裁罰案例(2/4)

■ 數位發展部成立後依照個資法裁罰案例

1 蝦皮購物

經數位部多次要求業者完善個人資料保護，並提出相關佐證資料以為證明，該蝦皮在個資盤點上仍僅提供4筆盤點內容，顯有缺漏，且在風險評估分析上，對於風險值較高之流程未提供已採取矯正措施之佐證。另外，對委外廠商未落實稽核，未能提供完整的安全管控執行、稽核紀錄等具體佐證資料，無法證實蝦皮對保有個資已採行適當之安全措施，因此依據個資法第48條第4款併第50條規定，處分業者併同其負責人罰鍰計新台幣20萬元

2 誠品生活

經數位部產業署實地行政檢查，現場已發現在帳號管理上執行未確實，另要求事後提供之補充或佐證資料，誠品公司個資盤點資料仍不完整，且針對委外廠商監督管理未落實執行，因此依據個資法第48條第4款併第50條規定處分，業者併同其負責人罰鍰計新台幣10萬元

3 旋轉拍賣

數位部說明旋轉拍賣已經提出說明及佐證資料，且已依先前包含警政署等專家建議，強化網站防詐警示、登入採用雙重驗證機制、並禁止用戶利用對話功能傳送未經驗證之網址連結等，惟未提供針對委外廠商整體制度稽核，尚有待改進之處，將限期請業者再行補正

行政責任裁罰案例(3/4)

- 行政裁罰案例： A網路書局

解除分期付款案件統計(107-108)

107.5.2 不通過 限期改善	107.9.12 不通過 限期改善	108.3.13 不通過 限期改善	108.7.23 不通過 限期改善
☒ 未落實個資保護管理程序。	☒ 未落實個資保護管理程序。	☒ 未落實個資保護管理程序。	☒ 未落實個資保護管理程序。
☒ 未落實白名單管理及進行log分析。	☒ 未落實白名單管理及進行log分析。	☒ 未落實白名單管理及進行log分析。	☒ 未落實白名單管理及進行log分析。
☒ 未落實個資外洩危機處理措施程序。	☒ 未落實個資外洩危機處理措施程序。	☒ 未落實個資外洩危機處理措施程序。	☒ 未落實個資外洩危機處理措施程序。
☒ 建立員工電腦與公司系統連線管控	☒ 建立員工電腦與公司系統連線管控	✓ 建立員工電腦與公司系統連線管控	
☒ 提升使用者密碼強度及變更密碼機制	☒ 提升使用者密碼強度及變更密碼機制	✓ 提升使用者密碼強度及變更密碼機制	
☒ 風險評鑑資訊清查	☒ 風險評鑑資訊清查	✓ 風險評鑑資訊清查	
☒ 辦理員工資安教育訓練	✓ 提供員工教育訓練		

行政責任裁罰案例(4/4)

●行政裁罰案例： A網路書局

- **行為一：違反個資法第48條第2款（舊法）**
  - ➢ ○○○公司是否已踐行個資法第12條通知義務
- **行為二：違反個資法第48條第4款前段（舊法）**
  - ➢ 就白名單管理與防毒軟體布署是否落實
  - ➢ 是否建立個資外洩之危機處理措施程序
  - ➢ 是否提出落實適當安全措施之紀錄與證據
  - ➢ 是否安排資安合約採購作業與提供執行弱點掃描、滲透測試與白箱原碼檢測輸出等成果文件，以佐證已改善或排除弱點
- **個資法第50條**
  - ➢ 代表人是否已善盡防止義務

個資法相關規定之說明(1/2)

個資法規定	說明
§2	客戶之交易個資屬於一般個人資料，應依個資法§2處理，並有適當之安全維護措施
§12、細則§22	公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人
§22	中央目的事業主管機關為執行資料檔案安全維護，認有必要或有違反本法規定之虞時，得請相關人員為必要之說明、配合措施或提供相關證明資料
§27Ⅰ、細則§12	非公務機關保有個人資料檔案者，應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏
§47	違反§6、19、20I、21者，由中央目的事業主管機關處五萬元以上五十萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰

個資法相關規定之說明(2/2)

個資法規定	說明
§48 I	違反§8、9、10、11、12、13、20II或III者，將由中央目的事業主管機關限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰。
§48II	違反§27I或II，由中央目的事業主管機關處新台幣2萬元以上200萬元以下罰鍰，並令限期改正，屆期未改正者，按次處新臺幣15萬元以上1500萬元以下罰鍰。
§48III	違反§27I或II，其情節重大者，由中央目的事業主管機關處新台幣15萬元以上1,500萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰。
§49	非公務機關無正當理由違反§22，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣二萬元以上二十萬元以下罰鍰。
§50	非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條規定受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰。

附錄-國際傳輸相關條文

- 個資法第21條。
  - 原則：不另設限制（但仍須符合蒐集、處理、利用相關規定）
  - 例外：

    非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之：

    一、涉及國家重大利益

    二、國際條約或協定有特別規定

    三、接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞

    四、以迂迴方法向第三國（地區）傳輸個人資料規避本法

附錄-國際傳輸的原則與例外

- 原則：許可
- 例外：中央目的事業主管機關得限制
  限制要件：國家重大利益/ 國際條約協定規定/ 接受國個資法規不完善/ 迂迴方式傳遞

- 通訊傳播業
- 金融業
- 醫院
- 社會工作師
- 蘋果日報
- 人力仲介業
- 西藥批發零售業

附錄-國際傳輸對通訊傳播事業之限制

- **應注意中央目的事業主管機關/個資專責機關是否有發布相關限制**
- **法務部107年8月21日法律字第10703511390號**
  - 國家通訊傳播委員會曾以大陸地區之個人資料保護法令尚未完備，限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區（參國家通訊傳播委員會101年9月25日通傳通訊字第10141050780號函）

Thank you